Report To The
Chief Judge Of The State Of New York

Commission on Public Access To Court Records
February 2004

EXHIBIT 3

RID - USA, Inc.
P.O. Box 520, Schenectady, NY 12301
(518) 393-HELP (-4357)
372-0034 FAX 370-4917

Testimony to the Commission on Public Access to Court Records
5-16-03 LOB Hearing Room C Albany, NY

Doris Aiken, RID-USA President & Founder

Good afternoon. I am Doris Aiken, Founder and President of RID (Remove Intoxicated Drivers) formed in 1978 to deter drunken driving and to serve and protect victims' rights.

Court records need to remain public and easily accessible in all formats including court dockets, DMV driving records, and on the Internet. The records need not show the addresses, social security numbers, banking or other personal I.D., but must include the full name, date of birth and court arrest and conviction records. If a violent crime (RID considers DWI a violent crime) then the record must stand for ten years. This is currently the law for DMV records if alcohol is involved in DWI/AI convictions.

Public safety and justice for crime victims are closely related to open records available to everyone. The unfortunate closing of driving records by Federal mandate several years ago due to a stalking incident in California where a starlet's address pulled from the DMV open driving records resulted in her being assaulted by a stalker, means that victims can only get needed records if a prosecutor is indicting someone. Often, in DWI fatal cases, if there is no alcohol involved in the defendant's record, the prosecutor can only look at a three year driving record. In one case involving the death of a 17 year-old pedestrian by an extremely drunk 22 year old in New York City, the prosecutor could obtain legally only the three year driving record. The court docket in the area where the drunk driver lived showed a history of reckless driving and speeding, as well as drunken property damage arrests. RID used its local volunteer court watch service to look at the local court records, giving this vital information to the prosecutor. Without public access to the court dockets, this criminal would have received a very light sentence, or just probation. The judge acknowledged the defendant's court record, read slowly at sentencing, which led to a 3-8 year sentence for manslaughter. Under current law, RID volunteers can obtain DMV driving records, but cannot use them to help victims, or prosecutors.

A better solution for the Federal mandate would have been to eliminate the address and other personal information from the public records, but letting stand the full name and DOB of the drivers. I recommend this solution to this Commission. People move a lot for various reasons. When I was called by a DWI victim's family from Connecticut whose daughter and new son-in-law were killed by a New York driver charged with a reckless plea bargain as a first time offender, I was able to check the local New York court docket. In this particular case, we were able to alert the prosecutor that the defendant had been charged with vehicular assault two years earlier, putting his victim into a coma. This changed the entire course of the adjudication process, and the surviving family saw the criminal justice system work. The defendant pled guilty which enabled the family to proceed with a civil suit without having to prove guilt. RID can no longer provide this service under the restricted rules for open records.

Open criminal and driving records are a public safety necessity on the Internet, as are cameras in the court. A minimal fee of no more than $5 could be charged for downloading Internet records. More could be charged for full text searches, but victims should have to pay nothing. They have already paid full measure for someone else's crime(s).

RID has audited and/or reviewed more than 11,000 court cases in New York alone since 1983.

Respectfully submitted by Doris Aiken.

Commission on Public Access to Court Records

Testimony submitted by
Michelle Rea
Executive Director, New York Press Association

May 16, 2003

Good Afternoon.
My name is Michelle Rea. I am the executive director of the New York Press Association, the trade association representing more than 600 weekly newspapers throughout the State of New York. NYPA's member newspapers include more than 400 community newspapers, almost 200 ethnic newspapers, a dozen business newspapers, and a dozen religious newspapers.

I also serve as the Senate Majority Leader's appointee to New York State's Committee on Open Government.

New York's weekly newspaper industry appreciates this commission's work, and is grateful for the opportunity to present comments regarding electronic access to court case records.

In an era when the law has become a fixture of popular culture, court administrators nationwide, understandably, are stepping gingerly into the age of Internet access to court records.

Electronic access to court records will be an important method of allowing meaningful public access. Denying public access to court documents that have always been open to the public, simply because they are now available in electronic form, would be devastating.

The practical implications of the transition from paper to electronic records can not be overstated. The public's right to access court records on paper at the courthouse is good in theory, but is a poor vehicle for uninitiated members of the public and journalists on deadline.

Electronic access to court records will be a great benefit to journalists, citizen and watchdog groups and the public at large. Electronic access should not be considered a luxury - it is a way to utilize court information in a meaningful way. Important public controversies can be tracked, statistical comparisons can be made, and relevant information can be quickly located when records are available electronically.

Members of the public, and journalists covering the judicial system will no longer be required to make a trip to the local courthouse to inspect or photocopy files. Members of the bench, the bar and the press will never again be frustrated to learn that a sought-after file is "out". No longer will journalists need to visit dozens of courthouses around the state to determine how drunk driving cases are handled in different jurisdictions.

No longer will reporters for morning papers be stymied when they pick up the last entry in the police blotter long after courthouse hours have ended for the day.

Computer-assisted reporting will permit journalists to quickly build spread-sheets to compare hundreds of cases, perhaps comparing companies with sexual harassment problems, or comparing sexual assault prosecutions, or the disposition of domestic violence cases. Court records that contain information about abuse in foster homes will enable reporters to quickly and thoroughly search names, addresses and other relevant details to determine whether foster parents have a record of abusive behavior.

Stated simply, electronic access to the same records that are currently available on paper, will permit journalists to do their jobs better, when precious deadline time is no longer spent finding, copying, and managing large quantities of paper files.

More importantly, journalists do their work on behalf of the public, recognizing that access is key to monitoring the legal system, to holding accountable those who work in the system, and to ensuring public trust in it. Journalists research, analyze and compile data gleaned from court records in an effort to ensure that members of the public know what goes on in New York's courts.

The commission asks if there are privacy concerns that should limit public access to court records on the Internet. Legitimate privacy concerns certainly exist for all of us. However, it is important to remember that neither the Legislature nor the Court of Appeals in this state has ever articulated any public policy in this state protecting against the disclosure of embarrassing private facts. /// That said, New York's courts do not want to become purveyors of truly sensitive information that serves no public purpose, over the Internet. Opening court records to the cyberworld places court administrators at an intersection where conflicting interests meet.

These competing interests will undoubtedly be difficult to resolve. The most satisfactory resolution will result in the creation of a standardized system that allows for access generally, and protection when needed in specific instances.

The commission must distinguish between concerns about the release of non-public information that could be used to inflict harm (for example, social security and credit card numbers, PIN numbers, or other information that could facilitate identity theft) from information that would simply be embarrassing if disclosed.
The extensive experience shared by the members of this commission undoubtedly renders them able to invoke a "common sense" test, to be used to protect confidentiality and security when necessary. "What would happen if the court disclosed?" is the key question, and the common sense answer is

usually correct. We believe two principles should guide the commission: first, the existing presumption of access should prevail, except for certain portions of unique personal identifiers, such as social security, bank account, and credit card numbers, which have no public or news value, and which if disclosed, could be harmful.

Second, there should be no different rules for Internet access to court records than exist for paper records at the courthouse.

Comparing public access to court records with the State's Freedom of Information Law may help provide a suggestion worthy of the commission's consideration. The FOIL statute's title, "Freedom of Information," is a misnomer for a law that actually provides access to records, not to information.
The New York Press Association urges the members of the commission to consider determining in advance which unique identifiers would always be out of bounds in the interests of avoiding harm, and to consider advising litigants on a uniform basis.

Perhaps the members of the commission would consider a systemic reform of the information required of litigants, revising the current procedures governing the creation and preparation of court records. If the court has a record, the record is subject to the rights of access. If however, no record exists, the question of access to the information ceases to exist.

New and emerging technologies will also provide simple solutions to some of the legitimate privacy issues. While I admit to being technologically challenged, I do know that software exists that can be used to block Internet disclosure of social security numbers or other personal identifiers in court documents. A simple coding process makes it possible to easily identify such data and to implement its exclusion.

Banks and other private businesses, including NYPA, have for years, utilized secure transmission software packages, which automatically code sensitive, classified information, preventing unauthorized people from accessing protected information.

Safeguards for unique personal identifiers should be imposed only where required to protect financial security and personal safety, not to avoid embarrassment. Litigants are using a public process when they go to court to resolve disputes, and access to all but limited facts is essential to allow public accountability over the process.

In withholding potentially injurious identifying information, NYPA urges the members of the commission to resist the temptation to permit case by case determinations, and instead, to establish a firm, system-wide, standard policy in advance, redefining the information litigants are required to provide, such as the disclosure of a unique personal identifier that is merely incidental to the issues brought before the court.
Additionally, the court must implement software to assure

appropriate electronic redaction when necessary.

The determination of which information is redacted from electronically accessed records should not be left to litigants and their counsel. Filing parties vary greatly in terms of resources, and should not be relied upon to discharge this responsibility properly.

Electronic access to court records will enable the public to track matters of public concern. Although drunk drivers might claim that they have a privacy interest in keeping their drunk driving history a secret - or at least available only at the courthouse - there is clearly a much stronger public interest in knowing how chronic drunk drivers are treated by the courts and in knowing whether our laws are fairly and properly enforced.

Even seemingly "private" disputes are of important public interest. Tort, shoplifting, sexual abuse and contract disputes are of public interest. Disclosure shows how the courts work, what standards are applied, and ensures that justice is being done.

The only "invasion of privacy" that courts need to protect against is that which truly can inflict injury. While it may be uncomfortable to know that one's neighbor has access to all the ugly details of a DWI case, and the tribulations of a problem drinker, this is not the type of compelling interest that should overcome the presumption of open records. There is always a public interest in knowing how courts decide these issues, what they consider, and what they don't. Rarely, if ever, is there a

public interest in one's social security number.

Responding to the commission's question regarding fees to be charged for access, NYPA recognizes that providing access to court records consumes precious court resources. Staff time today is required to maintain and provide public access to court records. Public access is not without public cost. The cost of access is either absorbed by taxpayers who fund the courts, or by those requesting access.

If records are available in electronic form, less staff time may be required to provide public access. Conversely, there will be costs associated with the conversion from paper files to electronic records.

The members of the commission must determine what level of access should be funded by taxpayers, at no cost to those seeking information. Any new fees that the commissions deems necessary should be minimal so as not to deter or restrict access.

Given that the court currently charges nominal fees for reproducing records, it is not unreasonable to expect that another nominal fee structure be implemented to ensure the court's ability to maintain an acceptable level of customer service.

Finally, the commission asks what format should be used to create and maintain electronic court records. The short, non-technical opinion offered by NYPA is that the commission

endeavor to implement system that makes electronic court records equally accessible to all computer platforms and operating systems. Recognizing the existence of a "digital divide," the implementation of a fully searchable, text-based system will level the playing field for those members of the public with limited computer skills or equipment.

The New York Press Association respectfully suggests that, should the commission be forced to consider creating and maintaining a log of electronic users, it carefully balance the practical inconvenience, intrusiveness and chilling effect against the potential uses and possible benefits of maintaining such a log.

It is reasonable to expect that in a short time, access to virtually all court records will be electronic, and to anticipate a time when paper archiving will become obsolete. NYPA recognizes that the ground-breaking work of this commission will not be easy, and we are grateful to Judge Kaye and the commission members for their ongoing efforts to ensure that the public's right to know what goes on in New York's courts is preserved.

Testimony of
Rex Smith
Editor and Vice President
Times Union
Albany, New York

Before the
New York State Commission
On Public Access to Court Records

Friday, May 16, 2003

The work you are undertaking is both complex and important. As we confront the realities of a digital age, it is essential that the institutions of American government at all levels strive to interact with citizens at a level appropriate to their expectations. And the expectation of an increasing share of our informed citizenry is that information will be available digitally and, generally, over the Internet.

Just as the invention of radio and television changed the way our politicians interact with their constituents – with the advent, first, of Franklin D. Roosevelt's fireside chats and then, later, John F. Kennedy's mastery of the televised press conference – so today must government reflect the reality of interactive communication by computer.

Courts have traditionally been slower than the other branches of government to engage openly with citizens, and for even rather proudly shielding the courts' work from public view. For example, a relatively small share of judges in this state allow cameras into their courtrooms absent a specific statutory requirement that they do so, although cameras have been an essential tool of communication for a century. And there has seemed to be an ethic in many courts that the dignity of the bench and the public's respect for its work will be maintained only if court proceedings and documents are shrouded from the prying eyes of citizens.

Fortunately, this commission's charter was set by a remarkable judge with a refreshingly different perspective. Chief Judge Judith S. Kaye is clearly committed to examining the tough issues of public access to both courtrooms and the records of the courts, with an eye to opening as much as possible to public view. It is a commendable objective, and one that I'm sure most journalists cheer. Of course, we expect no less from a jurist who started her career as one of us.

Oddly, perhaps, my industry might be presumed to have a commercial interest in maintaining the status quo – that is, in avoiding electronic access to court records. Reporters are more likely than average citizens to find the offices of court clerks and figure out how to retrieve ostensibly public information that is now available only on paper in court files. If we hope to preserve our role as the gatekeepers of public

information, perhaps we should recognize that Internet access to court records would take at least some of that power out of our hands. Why, you might ask, should citizens buy a newspaper to learn about what's going on if they can find it for themselves online?

But the great democratizing value of open access to court records far outweighs any financial incentive that newspapers might have to argue for what we have now, which is, in fact, a system of limited access that serves journalists better than it does our readers.

We recognize that some of those who testify before this commission will raise concerns about privacy. Those are real concerns, although the instances of harmful intrusions into ordinary citizens' private lives are really far less numerous than a lot of public policy worry-warts would have us believe. I am convinced that these concerns can be addressed by the regulations you propose. Essential privacy can be maintained while still offering Internet access to court files. That fear must not take precedence over the cleansing value of the light that electronic access would shed on the courts.

Fundamentally, we in the media would argue unanimously, I'm sure, that nothing in this commission's work should lead to a diminution of public access to the court records now available. That argues against a sort of two-tiered system that some would advance, in which certain categories of citizens would have more ready access to the files than others. To this non-lawyer, that sounds unconstitutional, anyway.

There is nothing to suggest that these privacy concerns can't be addressed by the litigants in a case themselves. That is, regulations could lay out categories of information that ought not to be disclosed online – such as Social Security and credit card numbers and other quite personal information – and the burden of preserving the confidentiality of that information could rest on the litigants. Most of the court documents that include information that rightly should remain confidential are not now available for public release, anyway. Litigants ought to be able to redact such confidential information from documents that would be filed, which then, presumably, would be scanned and made available electronically. It should not be the responsibility of the state to engage in such costly redaction. But this commission would need to make very clear that redaction could only apply to those limited categories it would establish. And, again, I would urge you not to remove from public access information that now is available in paper documents.

Nor does the concern about privacy mean that a system can't be established that might effectively discourage those who some imagine to be lurking, ready to snatch electronic court records for some nefarious purpose. Just as a Freedom of Information request provides a means of identifying who is drawing information from the files of the executive branch, an online registration could leave for the courts an identifying trail that would discourage those who some worry would be going after the records to commit a crime or disrupt someone's life. In addition, the system could be structured so that catch-as-catch-can searches wouldn't be possible, perhaps by limiting search terms to the names of litigants, the names of attorneys and index numbers, rather than full text.

Permit me, then, to describe some typical scenarios under which Internet access would be beneficial:

- A reporter hears in the late afternoon about a lawsuit filed in state Supreme Court involving a public official. Plaintiff's counsel is unavailable, and the official, as the defendant, offers what must be viewed as a self-serving "spin" on the situation. Since it's too late for the reporter to reach the courthouse and pull the case file, readers could learn about the allegations only if the reporter can call up the file on his office computer.

- A reader learns from a newspaper article about a class action lawsuit in which she thinks she may qualify as a member of the class. By going online to check the case files, she can find out firsthand about the case.

- At night arraignments in a city courtroom, a reporter is tipped that a defendant has a significant prior criminal record. A check of the court's electronic files reveals that, contrary to the tip, the defendant had been arrested but never convicted of a crime. An inaccurate and perhaps libelous article is thus averted.

Beyond these scenarios, of course, this commission's work offers a chance to enhance the role of the press in monitoring the court system. The press would gain a new tool toward meeting that responsibility with the electronic access that might make such review more aggressive and meaningful.

That might sound like an arrogant role for a bunch of journalists, mostly non-lawyers. But the watchdog role of the media is well established in our society, and it can be performed effectively only when responsible journalists gain access to the institutions of government. Your work can help make that possible.

We will be grateful for your efforts in that regard, and for all that you are pursuing on this agenda, as I am for your attention to this testimony. Thank you.

The Times Union, which is read by almost a quarter-million people daily, is the dominant information source in New York's Capital Region. It is one of a dozen newspapers owned by the New York-based Hearst Corporation, one of the world's largest diversified communication companies.

NEW YORK NEWSPAPER PUBLISHERS ASSOCIATION, INC.

120 Washington Avenue • Albany NY 12210 • 518/449-1667 • Fax: 518/449-5053

Diane Kennedy
President

Commission on Public Access to Court Records
May 16, 2003

Testimony of Diane Kennedy, President
New York Newspaper Publishers Association

Good afternoon, Judge Graffeo and members of the Commission. My name is Diane Kennedy, and I am president of the New York Newspaper Publishers Association. NYNPA is the trade association which represents the publishers of the state's daily newspapers. Our 54 member newspapers are read by more than five million New Yorkers every day. They range in size from *The New York Times* and *Wall Street Journal* to the *Adirondack Daily Enterprise* and *Hornell Tribune*, and span the state from *Newsday* on Long Island to the *Buffalo News* in the west and the *Courier Observer* in Massena to the north.

Our members provide their readers with an accounting of the actions of the legal system. Their reporting concerns both criminal and civil court proceedings, from town justice court arraignments for drunken driving to constitutional arguments before the Court of Appeals. The questions of law they present to their readers involve everything from public safety to product safety, from gun permit applications to taxpayer lawsuits against the state.

Few citizens have the free time needed to search court records for items of interest. Many, however, show great interest in learning about the legal system through stories prepared by our journalists. These citizens support the courts and the government through their tax dollars and are entitled to oversee their activities.

Providing the broadest and most affordable possible access to a wide array of legal documents helps to accomplish this purpose. As a report issued in October 2002 by the National Center for State Courts and the Justice Management Institute* found, access to court records promotes government accountability in at least three major areas 1) the operations of the judiciary, 2) the operations of other governmental agencies, and 3) the enforcement of laws. The report found that, "open court records allow the public to monitor the performance of the judiciary and, thereby, hold it accountable. Public access to court records allows anyone to review the proceedings and the decisions of the court, individually, across cases, and across courts, to determine whether the court is meeting its role of protecting the rule of law, and does so in a cost effective manner. Such access also promotes greater public trust and confidence in the judiciary. Openness also provides accountability for governmental agencies that are parties in court actions, or whose activities are being challenged in a court action. Finally, open court proceedings and open court records also demonstrate that laws are being enforced. This includes civil regulatory laws as well as criminal laws."

Our newspapers serve their readers by examining these court documents, sifting through reams of raw data and placing the findings in context. It is then up to our informed readers to voice their opinions about the information we have presented. Their opinions may result in a change in the administration of justice in their communities where necessary, and their involvement in this process can only serve to strengthen it. We agree with the National Center for the Courts study finding that, "open access serves many public purposes. Open access supports the judiciary in fulfilling its role in our democratic form of government and in our society. Open access also promotes the accountability of the judiciary by readily allowing the public to monitor the performance of the judiciary."

It is our position that the existing level of public access to paper court records should be maintained and may even be enhanced through digitization. The ability to efficiently search large numbers of court documents filed in courthouses throughout the state could enable newspapers to examine and report on important trends in the legal system, such as an increase in certain types of product liability proceedings. Dangers posed by products such as defective tires or health supplements containing the herb ephedra might have been disclosed sooner given enhanced court records access.

For this reason, we would urge the courts to adopt a system which would make possible full-text searches of electronic court documents. As the above-cited report notes, "one reason court records are publicly accessible is to allow the public to monitor the performance of the judiciary. One method of monitoring performance is to examine the information in a set of cases to see whether the court's decisions across cases are consistent, predictable, fair and just. This sort of examination requires access to all information considered by the court in making its decision, as it is difficult to say ahead of time that any piece or category of information is not relevant and therefore should not be made available."

We would also urge that the courts keep submissions up to date to ensure that our reporters are not presenting "stale" information to their readers. The courts should also do everything possible to ensure consistency in the digitization of court documents to ensure that there are not large holes in the array of records which are accessible. A failure to accomplish these two goals could result in our members inadvertently drawing incomplete or inaccurate conclusions from a compilation of court documents. We realize that these issues present great challenges, as there are variations throughout the court system in the form of filings and the way those documents are maintained.

Naturally, we are aware that significant costs could be attached to providing this level of access, and, given the state's current fiscal status, additional funding might not be forthcoming to offset these costs. Accordingly, the imposition of some form of fee for access might be necessary, although we would urge that any such access fee be set so as to offer the greatest possible access to New Yorkers of all income levels, and to journalists from even the smallest newspapers of very limited means.

We are also aware that the digitization of court records poses some privacy concerns, such as facilitation of identity theft. We recognize that a narrow range of data, such as social security numbers, credit card information and bank account information should be withheld, most likely through redaction. This might be accomplished by permitting litigants or their attorneys to redact a specified list of such data from filings before they are compiled and made available by the courts. Technology could also make it simple to redact some data through the inclusion of data "tags" on electronically prepared documents.

Data should never be redacted simply because it could be embarrassing to a litigant or some other participant in the legal process. The light of public scrutiny is intended to occasionally find faults in the legal system, and to cure those faults as expeditiously as possible.

On behalf of the New York Newspaper Publishers, I thank you for this opportunity to make our views heard, and for your interest in our opinions.

* "Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts" by the National Center for State Courts and the Justice Management Institute on behalf of the Conference of Chief Judges and Conference of State Court Administrators.

To: The Commission on Public Access to Court Records
From: Lisa Robert Lewis, editor, *The Record*, Troy
Re.: Testimony on putting court records on the Internet
Date: May 16, 2003

Your Honor, Mr. Chairman and distinguished members of the Commission on Public Access to Court Records:

It is a privilege to be able to address you on a matter that is of the utmost importance to newspapers throughout the state: Internet access to court records, and I thank you for your time.

My name is Lisa Robert Lewis, and I am editor of *The Record*, a 23,000-circulation newspaper prepared and published in Troy. *The Record* is part of the Journal Register Company, a major corporation based in Trenton, N.J., that operates almost two-dozen newspapers, primarily in the Northeast. In addition to *The Record*, JRC's New York State holdings including *The Saratogian*, The Oneida *Daily Dispatch*, the Kingston *Daily Freeman*, the *Community News* of Clifton Park, the *Independent* of Hillsdale and *The Taconic Press*.

I firmly believe in full and open disclosure of public records and that court records should be available on the Internet.

The Internet, as advertised, is indeed the information superhighway, and any roadblocks can only slow the progress made in providing important facts that all newspapers now use to enhance, enrich and make more accurate their reporting on matters of interest to the public. That court records are not currently accessible on the Internet is a roadblock.

At the heart of this matter is one simple fact: Court records are, and must always remain, public records, so denying easy Internet access is denying individuals and newspapers the right to use actual documentation in formulating an informed opinion on a criminal matter. Of course, newspapers and the public already have the right to access court documents, but as the members of this panel already know, that can be an expensive, time-consuming effort, an effort that not only creates difficulties for interested parties, but also ties up the time and equipment of understaffed courtrooms.

And for us at *The Record*, and at newspapers of a similar size, staffing and time constraints are legitimate issues.

Our larger colleagues in the Capital District and throughout the state have the luxury of staffing that allows one reporter to cover one case if it is important enough. For example, in our newsroom, one reporter might be covering court cases in Albany, Troy and its environs all at the same time. As a result, research time — time to examine records on a court clerk's schedule — is a luxury we can't always afford on a day-to-day basis.

And while this might seem a self-serving argument, when newspapers the size of *The Record* are able to do a better job covering the courts, it is, ultimately, the public that is served. While the economic realities facing small daily and weekly newspapers are not the responsibility of this Commission or the courts, the reality is that the combined circulations of these small dailies and weeklies across this state must be taken into consideration as a tremendous readership could be deprived of timely information.

The members of this committee will hear arguments against Internet access to court records, mostly centered on the right to privacy. The simple fact is that in New York state, there is no right to privacy written into law. A person's name or image can't be exploited for commercial purposes, to be sure, but that is the only guarantee afforded by law in the state. Perception of a common-law right to privacy is consistently rebuffed by the state's courts.

Naturally, there is a difference between what is legal and what is right, and exploiting a person's privacy is not the right thing for anyone to do. But what goes on in an open court of law is not privileged information; it is the right of all to see it.

And let's be bluntly honest. If someone wants information on another person, no matter how private, it is out there already. Free websites call only for a name and a general locale to come up with an address and telephone number in a matter of seconds. If a person does any commerce on the Internet, and an increasing number of us do, your Social Security number is out there for unscrupulous hackers with just a touch of technical know-how to tap into.

We believe, however, that Internet access to court records does not add to this problem. As I previously stated, court records are already a matter of public record. Making them more readily accessible would represent growth in the relationship between courts and the public.

The Internet itself is cluttered with unwanted email solicitations and pornography, and to some it represents an evil in our society. But just as television in its formative years, the Internet has incredible potential to create a better-educated society, one that understands the courts and the decisions made on a virtually daily basis that have major impact on our daily lives. Access to court records would help the Internet realize its potential, simultaneously serving the public.

Personally, I am very pleased that Chief Judge Judith Kaye appointed a commission to study Internet access to court records, as it is bound to create a healthy debate and air all sides of a vitally important issue. We hope the commission, when weighing its recommendations, looks beyond the few minor, fixable problems that could occur with Internet access to court records and sees how valuable a tool this access would be to newspapers and the public at large.

I thank you for your time and the opportunity to join in the debate.

Submission to the New York State Commission on Public Access to Court Records by the Ad Hoc Subcommittee on Internet Access to Court Records of The Association of the Bar of the City of New York

This submission is made in response to the Notice of Public Hearings of the New York State Commission on Public Access to Court Records (the "Commission") by the Ad Hoc Subcommittee on Internet Access to Court Records (the "Subcommittee") of The Association of the Bar of the City of New York (the "Association").[1]

The Purpose of This Submission

The purpose of the present submission is not to offer value judgments or definitive answers to the important questions that the Commission has been asked to study. Rather, the purpose of this submission is to share with the Commission the results of the Subcommittee's investigations and factual inquiries into the present status and future potential of Internet access to court records, which we believe may be helpful to the Commission in its deliberations.

Two preliminary observations are offered to provide context to our observations. First, although a framework for addressing confidentiality and

[1] The members of the Subcommittee are drawn from various interested committees of the Association, including the Council on Judicial Administration and the Committees on Communications and Media Law, Federal Courts, Government Ethics, Information Technology Law, and the Judiciary. The members of the Subcommittee are Sandra Baron, Terryl Brown, George M. Donahue, Joseph H. Einstein, Lori Goldstein, Marc Greenwald, Rajesh James (Secretary), Stephen D. Kahn, Alfreida B. Kenny, Todd L. Mattson, Michael Mills, Lynn K. Neuner, Robert C. Newman, Diana D. Parker, Richard J.J. Scarola, David B. Smallman, and Guy Miller Struve (Chair). While this submission is joined by all of the members of the Subcommittee other than Sandra Baron and David B. Smallman, it does not necessarily fully reflect the views of the individual members or those of their respective committees.

security of information already exists in the New York Court system, this submission is intended to explore whether such a framework can and should be applied to Internet access to court records. Second, in making this determination, it is necessary to balance privacy and security interests on the one hand with rights of public access on the other. The benefits of public access are clear. Therefore our submission focuses on the countervailing interests and asks whether these should limit presumptive access rights.

The Present Scope and Future Potential of Internet Access to Court Records

In considering the issues before the Commission, we believe that it is helpful to bear in mind that the present scope of Internet access to court records falls far short of its future potential.

With the technological means available today, it is feasible to implement a system of unlimited public Internet access to court records in which any person anywhere in the world who had access to the Internet could carry out a full-text (i.e., "Lexis-type" or "Westlaw-type") search throughout all the court records available on the Internet for a given search term (which could be a person's name, address, telephone number, credit card number, or date of birth, or any other search term). Such a search would locate any court records accessible anywhere on the Internet that contained the chosen search term (for example, that mentioned a chosen name), whether it was part of the caption of a case, or was just mentioned incidentally in the course of a trial transcript or in the middle of an exhibit submitted to the court. As described more fully in our response to the

Commission's Question 1 below, such a system of full-text access to all court records could raise issues of privacy and security.

Such a system of full-text Internet access to court records does not appear to be generally available to the public anywhere in the world today. In the first place, many existing systems of Internet access to court records (including the Federal system) are not open on an unrestricted basis to all Internet users, but require users to obtain and use passwords to gain access. As a matter of business policy, existing full-text Internet search engines (such as Google.com and Yahoo.com) do not index (and therefore do not offer full-text searches of) Internet sites that are available only to authorized users. For this reason alone, most existing systems of Internet access to court records are not candidates for full-text access.

There are some systems of Internet access to court records that are not limited to authorized users, but that are open to all users of the Internet.[2] A well-known example is Hamilton County, Ohio (the county in which Cincinnati is located), which initiated full Internet access to court records in late 2000. The Hamilton County web site has generated both extensive usage and significant controversy.[3] It does not, however, offer full-text search capability of the

---

[2] One such system is the New York State E.Court system, which offers Internet access to court calendars, orders, and opinions in certain cases. This system, however, does not presently offer access to all court papers filed in the cases it covers, and does not presently enable full-text searching.

[3] Our understanding is that legislation is under active consideration in Ohio to address various concerns raised by Internet access to court records.

contents of documents, but only allows users to search by case name, docket number, and names of counsel. A full-text search capability does not exist within the Hamilton County web site itself, and commercial vendors do not appear to have indexed the contents of the web site in order to provide such a capability.

Thus while Internet access to court records is still relatively new, and while this Subcommittee cannot state with certainty that it has reviewed all of the systems available to date, the capability of carrying out full-text Internet searches of court records does not appear to exist anywhere in the world today. However, if a given body of court records (for example, those in New York State) were to be opened to unrestricted Internet access, then it would automatically become technologically feasible for commercial vendors to copy and manipulate such records, thereby providing full text search capability regardless of whether or not the court system itself chose to provide such a capability as part of its web site. Alternatively, large litigants or law firms could set up proprietary systems allowing full-text searches which would not be available to other lawyers or litigants or to the public at large. This fact raises considerations of equality of access to public records that the Commission may wish to address.[4] It also suggests that the issues that would be raised by full-text searches of court records need to be considered before implementing any system of unrestricted Internet access to court records.

[4] For example, courts might provide records directly to the public or might contract out to services such as Lexis and Westlaw for that purpose. Further, courts may choose to create rules regarding permissible downloads from their own sites. Such rules could require monitoring by court personnel and sanctions for misuse.

Against the background of the foregoing facts, the Subcommittee offers the following responses to the questions posed by the Commission.

1. In light of the recognized public interest that is served by having court case records available for public inspection, are there any privacy concerns that should limit public access to those records on the Internet?

The Subcommittee fully concurs with the Commission that there is an extremely important public interest in having court records available for public inspection. In the case of many court records (including trial records), this public interest is of constitutional dimension. Public access to court proceedings is vital to public confidence in the fairness of the judicial process.

The Subcommittee believes, however, that there are certain countervailing interests that should be weighed against the constitutional and common law access rights in considering the implications of unrestricted Internet access to court records. The matters that come before the courts for resolution include the most intimate, private, and painful aspects of people's lives. Although many of these are already matters of public record accessible to those interested in taking a trip to the courthouse, to open all court records to full-text searching would open all of these matters to unrestricted browsing at the click of a mouse by people throughout the world.

The countervailing interests include not only privacy interests, but security interests – the interests in physical and financial security. To the extent that unrestricted Internet access to court records included private financial data of individuals, it could be used in such a manner as to threaten their financial

security (for example, by identity theft). And there are individuals affected by court proceedings whose physical security may also be at stake if court records can be used to trace their present whereabouts, or to find out how the rooms in their dwelling place are configured.

Although a limited portion of the information at issue may already be available online, unrestricted Internet access to court records, especially with full-text searching, is qualitatively different from anything that is generally available today. Full-text Internet searching is far cheaper, and far more powerful, than manually searching records at a courthouse on a file-by-file basis. Other differences also exist. For example, while users of courthouse files typically are not required to identify themselves in order to obtain and review such files, the fact that users must appear in the courthouse in order to access court records (and therefore may later be subject to identification by courthouse personnel) may serve to deter some who would seek to use the information in court records for improper purposes.

2. Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the Internet by the Unified Court System? For example, when public court records contain an individual's Social Security identification number, credit card numbers, bank or investment account numbers or other personal identifying information, should privacy concerns limit their disclosure on the Internet?

For the reasons summarized in answer to Question 1 above, the Subcommittee believes that, before unrestricted Internet access to court records is implemented, consideration should be given to whether or not such access is appropriate in the case of categories of information that may pose concerns with

respect to personal privacy or security.

The types of personal identifying information listed in Question 2 are obvious candidates for scrutiny from this point of view, but they are not the only categories of information that deserve consideration. Among the types of cases that courts and/or committees in other jurisdictions have deemed worthy of special consideration (some of which are already subject to statutory seals in this State, at least to some extent) are custody cases, juvenile cases, matrimonial cases, mental health proceedings, and probate cases. Other types of cases that would not ordinarily pose privacy or security problems may raise such problems in individual cases.

In noting that such cases may raise issues that are worthy of consideration, the Subcommittee is not prejudging or advocating that Internet access should be blocked in any or all such cases. In general, the Subcommittee believes that any restrictions on Internet access should be the minimum necessary to prevent significant harm to privacy or financial or physical security.

In weighing privacy and security concerns, it should be borne in mind that the efficiency and power of full-text search techniques will seek out and reveal even a single instance in which sensitive information has inadvertently been left open to Internet access, even if all other occurrences of the same information have been successfully blocked from access.

3. If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic/Internet availability?

For the reasons summarized in the answer to Question 2 above, the

Subcommittee does not believe that the privacy and security concerns raised by unrestricted Internet access to court records are limited to personal identifying information. For this reason, our answer to Question 3 embraces all types of personal information that might ultimately be judged worthy of protection for privacy or security reasons.

To the extent that particular categories of cases or particular cases were to be excluded from unrestricted Internet access for privacy or security reasons, it would be relatively easy to identify the cases to be excluded from Internet access and to implement the exclusion. For example, particular types of docket numbers could be used to identify such cases, and cases bearing those docket numbers could be excluded from unrestricted Internet access.

To the extent that a decision were to be made instead that particular types of information should be excluded from Internet access while the rest of the document in which such information is found remained open to Internet access, the implementation of such a decision would be more difficult. The problem is not primarily a technological one. Means will shortly exist in widely-used word processing software by which particular information in a document (such as a bank account number) can be "tagged" with an electronic indicator that could be used to exclude that information from Internet access.[5] The problem, rather, would lie in making sure that the "tag" was affixed in all cases in which it was

[5] One such means would be the use of XML (Extensible Markup Language) codes to "tag" the information in question.

supposed to be affixed. This problem is addressed in Question 4 below.

4. If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys or by others?

Again, as in the answer to Question 3, to the extent that the decision was made that particular categories of cases or particular cases should be excluded from unrestricted Internet access, it would be relatively straightforward to implement such a decision. The responsibility could be placed in the first instance on the parties (subject, if appropriate, to court review) to indicate whether or not a given case belonged to one of the categories in question. Such cases could be given distinctive docket numbers, and the system of Internet access could be established in such a manner as to exclude such cases from access. Greater ease of administration must, however, be balanced against an inherent decrease in sensitivity to both privacy and public access interests. While the exclusion of entire categories of cases is relatively easy to implement, like any categorical rule such exclusion would be both under and over inclusive with respect to private information.

To the extent that a decision was made instead to require that particular types of information be "tagged" and excluded from Internet access, it would be unrealistic and inappropriate to place the burden of identifying and "tagging" upon already overburdened courthouse personnel.

As a practical matter, it would probably be necessary to place the burden of identification and "tagging" in the first instance upon the party filing such information, perhaps with some form of required certification. Unfortunately, it

would not always be the case that the filing party had both the resources and the motivation to discharge this burden properly. In particular, there might be problems with adherence to these requirements on the part of pro se litigants.

The only remaining alternative would be to rely upon the adverse party to check that the filing party had discharged its obligation (and, perhaps, to postpone Internet access for a few days to allow this check to be made). This would require a high degree of alertness on the part of the adverse party, and even this would not necessarily protect sensitive information of a third party which neither the filing party nor the adverse party had any incentive to protect.

Realistically, we believe that any system of identifying and "tagging" particular information for withholding from Internet access is likely to be imperfect. And, as noted at the end of our answer to Question 2, because of the power of full-text search techniques, even a single slip could result in the sensitive information becoming public.

5. Should the public be charged a fee to access court records on the Internet?

In principle, because of the importance of public access to court records, the Subcommittee believes that user fees for such access should be avoided if at all possible, and that if they are to be instituted, they should be strictly limited to an amount sufficient to cover the marginal costs of Internet access (not the costs of the electronic filing system itself, which are more properly viewed as part of the underlying costs of the court system).

Moreover, as a practical matter, if user fees were to be instituted, the likely

result would be to encourage users to subscribe to the services of commercial vendors which would download the contents of the courts' web sites, and then charge lower fees (or no fees at all) for accessing them.

6. What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or index number, or some other limited method, or should full text searches be available?

For the reasons set forth at the outset of this submission, full-text searches raise more serious privacy and security concerns than do searches limited to the captions and docket numbers of cases.

As a practical matter, however, as noted at pages 3-4 above, once unrestricted Internet access to court records was available, even if the courts themselves did not make full-text searching available, commercial vendors could index the contents of the courts' web sites and make full-text searching generally available, and large litigants and law firms could perform the same functions for themselves.

May 2003

ADDITIONAL STATEMENT BY INDIVIDUAL MEMBERS OF THE AD HOC SUBCOMMITTEE ON INTERNET ACCESS TO COURT RECORDS OF THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

This additional statement is submitted by individual members of the Ad Hoc Subcommittee on Internet Access to Court Records (the "Subcommittee of The Association of the Bar of the City of New York (the "Association").[1] We write separately to underscore certain principles we believe should guide this Commission as it considers the application of new technology to the records maintained by the courts of this State.

INTRODUCTION

As the Subcommittee's Submission notes at the outset, clear benefits flow to society from our long history of public access to court records. We wish to stress the established legal framework for addressing access and the significant potential advantages that can be gained by Internet access to court files.

Internet access to electronically filed court documents offers an extraordinary enhancement to the public's ability to monitor and engage itself with the court system. Many individuals and groups monitor and rely upon public court files today – from the parties to litigation themselves, to the press, to watchdog and citizens' groups, to the public at large. Among the virtues of Internet access is that those who wish to review court records could do so without the limitations of court business hours, without the drain on the time of court personnel, and without the burden and expense of traveling to the courthouse and locating records. The advent of electronic filing offers very real and important opportunities.

Legitimate worries about privacy and security for information available on the Internet deserve full and focussed discussion. But, this discussion should proceed with

---

[1] The members joining in this submission include Sandra S. Baron, Richard J. J. Scarola, and David B. Smallman.

full recognition of the ground rules for resolving the tensions between access and privacy that have been established by the courts and the legislature of this State:

- Most court records are presumptively open for public inspection, a presumption that is protected by the constitution, statutes, rules, and common law of this State.[2] The courts of this State have extensive experience protecting confidentiality and security within the limits appropriately required by the public interest in access to court records.

- The Court of Appeals of this State has never recognized a tort for public disclosure of embarrassing private facts, and the legislature has never adopted a statute to protect this aspect of "privacy." It is therefore important to distinguish concerns about the release of non-public information that could be used to cause damage (*e.g.*, credit card numbers or bank account information that could facilitate identity theft), from information that would be embarrassing if widely disclosed.

The existing legal framework has developed over centuries. It reflects the hard lessons learned through long experience. That experience has taught us that the benefits of public access to information should not lightly be restricted. The application of new technology is not an occasion to reject the lessons of history.

We write separately also to underscore the fact that the same developing technology that is making possible electronic access to court documents, may itself offer innovative technological assistance to resolve many, if not all, of the legitimate privacy and security issues raised. For example, software already exists that can be used to block Internet disclosure of social security numbers or other personal identifiers in a court document. The process involves a simple coding that can be required to be included when a document is filed

---

[2] *See, e.g., Danco Laboratories, Ltd. V. Chemical Workers of Dedeon Richter, Ltd.*, 274 A.D.2d 1, 6, 711 N.Y.S. 2d 419,423 (1st Dep't 2000) (recognizing constitutional right of access to court records in civil proceedings); NY Uniform Rules of Trial Court 216.1(a)

with the court.

In addressing these issues, we urge the Commission to consider the rules for public electronic access to court cases that are already being adopted by the federal courts in New York. There is a benefit for counsel to proceeding on a uniform basis, to ease the adjustment to electronic filing and access.[3]

With these initial comments, we provide the following additional responses to the specific questions posed by the Commission:

1. In light of the recognized public interest that is served by having court case records available for public inspection, are there any privacy concerns that should limit public access to those records on the Internet?

We agree with the Commission that there is an extremely important public interest in having court records available for public inspection. As the Subcommittee Submission states, public access to court proceedings is vital to public confidence in the fairness of the judicial process. As noted above, we also underscore the absence of a public policy in this State generally protecting against the disclosure of embarrassing private facts.

The implications of such a legal constraint on newsgathering, and on the legitimate public interest in a free flow of communication, have wisely constrained the courts to enter sealing orders on a case by case basis. We would thus urge the Commission not to

---

(requiring consideration of public interest before any court record is sealed).

[3] Helpful guidance is available from recommendations on civil and criminal electronic case file availability and Internet use issued by the Judicial Conference of the United States, and in the recent enactment of the E-Government Act of 2002, which require federal courts to provide greater access to judicial information over the Internet, while promulgating rules to protect legitimate privacy and security concerns.

embark on the dangerous road of determining in advance what categories of information are inherently so sensitive or embarrassing that they deserve legal protection against disclosure on the Internet. Safeguards for information on the Internet should only be imposed where required to protect financial security and safety, not to avoid embarrassment or shame.

We urge that concerns about privacy for electronic records are best dealt with in same manner as courts in this State currently mange them in connection with paper records. There might well be countervailing interests to public access that present themselves in a given case, and we have little doubt that Internet access may heighten litigants' interests in pursuing the sealing of documents to a greater degree than currently exists in a paper record world.[4] However, there exist adequate standards and procedures available to litigants and others to request the sealing of information that it confidential and warrants continuing protection. *See, e.g.*, 22 NYCRR 216.1. The courts are experienced in balancing the interests appropriately on a case by case basis, and there is no reason they can not continue to do so with electronic records.[5]

---

[4] Without downplaying such legitimate concerns, much of the information that might be most problematic is readily available from other sources already. *See* Amitai Ezioni, THE LIMITS OF PRIVACY *10* (1999) ("Consumers, employees, even patients and children have little protection from marketers, insurance companies, bankers and corporate surveillance"). Indeed, the anecdotal research by members of the Subcommittee confirmed that a great deal of information, including social security numbers, was easily obtainable from Internet research tools by others on the Subcommittee. One question that is not being asked by the Commission, but that perhaps should be looked at, is whether the courts ask for personal identifying information in instances where it is not necessary and when other, less potentially problematic, identifiers could be used. *See, e.g.*, J. Cissell, *Privacy and Court Records on the Internet,* THE JUDGES' JOURNAL 29-30 (Summer 2001).

[5] We are assuming that the court websites will make available documents on a going-forward basis. The only fact submitted to the Subcommittee with respect to past documents from closed

2. Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the Internet by the Unified Court System? For example, when public court records contain an individual's Social Security identification number, credit card numbers, bank or investment account numbers or other personal identifying information, should privacy concerns limit their disclosure on the Internet?

For the reasons summarized in answer to Question 1 above, we do not believe that there should be different rules for Internet access to court records than exist for records at the courthouse. This is the policy decision that the federal courts have made and we believe it is wise.[6] That said, we recognize that the federal courts are recommending that full social security numbers, dates of birth, financial account numbers and names of minor children be excluded from electronically available records even for the bankruptcy courts which have been making such information available for some time. However, not all such identifiers in all instances require confidentiality. Hence, we again urge that case by case determinations are the best means of balancing the public's right of access to court records against specific and recognized privacy and security interests.

Any decision on Internet access should also take into account the extent to which personal information is already available over the Internet from other sources. Phone numbers, addresses, political party affiliation, mortgage indebtedness, the name of one's bank,

---

cases was that such documents would likely not be made available electronically. To the extent that the court system does plan to scan in records from cases that are closed, consideration may need to be given to a system of notifying the parties and provision for their reviewing and requesting redactions.

[6] *See, e.g.*, News Release, Administrative Office of the U.S. Courts, September 19, 2001 (<http://www.uscourts.gov/Press_Releases/index.html>).

and vast amounts of other pieces of "private" information are already available on-line. Public access to court records should not be limited in the interest of privacy, if the limitation is ineffective and serves no useful purpose. Any restrictions on electronic access should be effective in protecting against the perceived harm, and should satisfy the existing legal standards for sealing court records.

While we recognize that litigants themselves may question the increased scrutiny of personal identifying information disclosed in court records that are made available on the Internet, these concerns, where well-grounded, can be met by appropriate coding to permit the "electronic redaction" of information, as we discuss in response to the next Question.

3. If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic/Internet availability?

To the extent that personal identifying information should be excluded from unrestricted Internet access for privacy or security reasons, technological advances may make it relatively easy to identify such data and to implement the exclusion. Means may well exist now within commonly used word processing software, and more sophisticated means will shortly exist in widely used word processing software, by which particular information in a document (such as a bank account number) can be "tagged" with an electronic indicator that could be used to exclude that information from Internet access. The Commission will undoubtedly hear from those far more technologically proficient than we, and the means by which tagging can be effected should be explored.

4. If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys or by others?

The means by which information is redacted from Internet access of records will, undoubtedly, largely be the responsibility of the litigants and their counsel. The court's computer system would have to be configured to read the tags that the litigants would be required to place on documents in order to identify and electronically redact information from web access.

Identification and "tagging" in the first instance would be the responsibility of the party filing such information. While it has been noted that the filing party might not always have both the resources and the motivation to discharge this burden properly, this problem also exists with records available at the courthouse. We would suggest that a means for impressing upon counsel the need to manage the tagging system appropriately would be some form of required certification to the court on the issue; inappropriate disclosures would be subject to existing laws or rules that provide sanctions for such conduct. Adherence to these requirements on the part of *pro se* litigants may pose special problems as they always do, and some form of assistance at the courthouse would likely be necessary.

Again, the federal courts noted that with respect to the burden their proposed systems would place upon counsel and litigants, the courts – and we would add, undoubtedly with the assistance of the states' bar associations and continuing legal education institutions – might well have to undertake some means to educate the bar and the public about the fact that information will be available online and the means by which it can and should be protected. This educational process could go both to the need for parties to protect their own

identifying or other information appropriate for sealing, as well as the requirements imposed for protecting such information of others.

Realistically, we believe that any system of identifying and "tagging" particular information for withholding from Internet access may initially be imperfect. However, the situation is likely to improve as lawyers become more familiar with the practice. In addition, when lapses are identified, systemwide modification can occur with little delay if an appropriate mechanism is set up for corrective action. Finally, at least with respect to lawyers, having to certify to the court that he or she has met his/her obligations to implement masking of specified data is likely to impress upon lawyers the seriousness of their responsibilities on this matter, and that sanctions could await counsel who took such obligations lightly or intentionally made such information accessible in his/her filings.

5. Should the public be charged a fee to access court records on the Internet?

We agree with the Subcommittee's response with respect to fees. While, of course, not binding on the state courts of New York, it may be worth noting that in December 2002, President Bush signed into law the E-Government Act of 2002, which now mandates that the Judicial Conference "may, only to the extent necessary, prescribe reasonable fees" for collection by the courts for access to information available through automatic data processing equipment. The Senate Report accompanying the legislation observes that: "The [Senate Committee on Governmental Affairs] intends to encourage the Judicial Conference to move from a fee structure in which electronic docketing systems are supported primarily by user

fees to a fee structure in which this information is freely available to the greatest extent possible."

6. What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or index number, or some other limited method, or should full text searches be available?

Unless the court system is going to establish limits on the degree to which a user can download records from the system it establishes, it is our understanding from the information presented to the Subcommittee that a user could, theoretically, download the entirety of the records (or any significant and/or identifiable body of them) and render them full text searchable either for the user's own benefit or as a commercial venture. The Subcommittee received information that suggested that the cost of managing this was not so substantial that it would deter a user such as a large law firm from doing just that for its own benefit. [7] Whether due to cost in setting up the system, or concerns about security of the

[7] As the Subcommittee Submission states, if the courts themselves do not provide full text searchability, but allow private concerns to do so, there will likely arise issues of equity in terms of public access. One manner of addressing the issues of equality of access is for the court system itself simply to provide court records in a technologically sophisticated manner to all to whom it authorizes access, whether that ultimately is the public or authorized users. A related alternative would have courts contracting out to services such as Lexis and Westlaw to accomplish the same end, but providing for reasonable rates that would presumably make access reasonably and broadly affordable. While theoretically access could be conditioned on the user's agreement not to download the entire contents for this purpose, the fact is that rules would then also have to be developed that somehow determined what amount of downloading was too much (*e.g.*, one case, ten cases, twenty cases) which in turn would require monitoring by court personnel backed up by sanctions for misuse. One reality that the research of the Subcommittee has revealed is that increasingly greater quantity and quality of access or access capability is inevitable, and the only material question is on what terms.

system,[8] or concerns about securing the confidential data in the systems, no court system to our knowledge has, as yet, offered a full text searchable system open, without password or other limitation, to the public.

Full text searchability would allow for research into the number and disposition of categories of cases, of great use to press, scholars and those who monitor courts and their management more generally. It is among the great benefits of electronic record keeping.

It would require those who have information they believe should be confidential to take steps to insure that is managed. But to deny the public overall the benefits that could accrue as a result of full text search capacity because of fear of litigant error or misdeed would be short sighted and, in light of the exponential developments in computer technology, likely short lived.

May 2003

---

[8] The Subcommittee spoke by teleconference with Judge James Cissell, who as Clerk of the Court of Hamilton County, arranged for that court's electronically stored documents to be placed on a website, accessible by the public on the Internet. He told the Subcommittee that the reason Hamilton County had not adopted a full text searchable system was that at the time they felt the costs were too great and had been advised that it would allow the system to be more easily sabotaged.

Submission of the Office of the
New York State Attorney General to the
New York State Commission On Public Access To Court Records

(Testimony of Kenneth Dreifach, Chief,
Internet Bureau, Office of Attorney General, May 30, 2003)

The below testimony is respectfully submitted by the New York State Attorney General, in response to the Notice of Public Hearings of the New York State Commission on Public Access to Court Records (the "Commission").

1. The Purpose of this Submission

The Attorney General recognizes at the outset that court records are presumed public, and that vital public purposes are served by this tradition. Nonetheless, this Commission has the difficult task of balancing the traditional values of open records against real, practical concerns arising from the capabilities of new technology. As the former values are well-documented, we address only the latter, which reflect recent developments and trends.

The purpose of this testimony, however, is not to prescribe the precise balancing that should be undertaken as to these competing factors, or the specific procedures that should be implemented. Those determinations, of course, are for the Commission. Rather, we undertake merely to outline certain of the privacy and security interests that the Commission may wish to consider, such as the frequent use of personal information for identity theft or other potentially harmful activities.

We address two similar but distinct concerns, those of "security" and "privacy." In reaching its conclusions, we ask that the Commission consider basic security concerns that arise when personal identifying information is easily available to identity thieves – *e.g.*, data reflecting

banking information, social security and credit card numbers, or other similar personal and financial identifiers. But we also ask that you consider the independent concerns relating to sensitive information (such as medical, family, or other personal data) contained in court records, whose disclosure to information brokers may have undesirable practical consequences.

Any system that vastly broadens public access to these types of personal information -- as digitization and universal access unquestionably do -- should contain some effective means to safeguard such information. Otherwise, we risk chilling the public's willingness to access the court system, and even to assist the ends of justice.

2. Background: The Personal Data Identity Thieves Use, and How They Use It

The incidence of identity theft rises each year. Some 500,000 cases occurred in 2002, and this number will continue to rise. All consumers, rich and poor, are susceptible to this crime. Moreover, victims may not be made whole (*e.g.*, by the financial institutions involved) when someone hijacks their assets, identity, or information.

Identity thieves often combine "high value" personal identification, such as bank account or social security numbers, with "low value" information more readily available to the public, such as name, address, or birth date. Along this spectrum lies other data, readily available about some people, but not others: for instance, a prominent attorney's mother's maiden name, might be listed in Who's Who in America, along with his place and date of birth and his children's names (which may make his password easy to guess, as well); a CEO's signature might be accessible for forgery from her company's annual report (as attorneys' signatures are available in scanned PDF documents online).

Court records often contain the type of information most often used in identity theft,

especially records in consumer cases or class actions. Sophisticated corporate litigation records also may contain high-risk information: for instance, settlement papers may even list the bank account into which funds are to be wired.

Most obviously, accessible credit card information places consumers at risk. With it, a thief can order goods over the Internet, or launder money through an online payment aggregator. However, while many people consider credit card theft their major identity theft risk, it is far from the most pernicious, since the Fair Credit Billing Act and other laws traditionally have protected cardholders from most types of fraud.

The exposure of consumers' banking information causes even greater risks. With little more than a copy of your check (and thus your account number) an identity thief can scan, forge and cash checks in your name, and even set up a bank account into which to deposit (in your name) ill-gotten funds. In fact, simply knowing where you bank may be enough for a savvy con artist to trick you -- via emails and phony web site links that urge you, for "security purposes," to re-enter their account and PIN information through a phony web site – usually a copy of the your actual bank's web site.

The exposure of social security numbers also places consumers at risk, given the number's status as a universal personal identifier. With a social security number, an identity thief usually can, for instance, obtain a birth certificate. And with these, the thief can obtain (or convincingly counterfeit) your passport, utility bill, or a replacement driver's license.[1] He may

---

[1] See also Greidinger v. Davis, 988 F. 2d 1344, 1353 (4th Cir. 1993) ("Armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck.").

also access your financial assets, which often use your social security number as a *de facto* password and identifier. What then follows is limited only by an identity thief's energy and creativity: transferring funds, opening new bank or telephone accounts, obtaining multiple credit cards, car loans, and internet service accounts. (A savvy identity thief might even call the local phone carrier and unlist your telephone number – to make it more difficult for the thief's creditors to call you.)

Social security numbers are available for purchase from some online vendors.[2] However, this practice has been widely criticized, and there is a vigorous effort in Congress to ban or severely restrict these sales.[3] Further, the New Hampshire Supreme Court recently held that one such information broker, Docusearch, violated a common law duty when it sold a stalker the social security number and workplace address of his target, Amy Boyer, whom he then fatally shot at her workplace.[4] That court reasoned that "a person's interest in maintaining the privacy of his or her SSN has been recognized by numerous federal and state statutes. As a result, the entities to which this information is disclosed and their employees are bound by legal, and

---

[2] Some prominent Americans' social security numbers are already available in publicly accessible government databases. A cursory search on the EDGAR database (available both at sec.gov and on LEXIS/NEXIS) uncovers the social security numbers of some business executives, whose social security numbers appear on filings with the SEC -- stock agreements, reporting statements, employment agreements, and the like. However, in many other instances within that database, it appears that this information either was redacted or not placed online.

[3] For instance, the pending Social Security Number Misuse Prevention Act (S. 228, H.R. 637 sponsored by Sen. Feinstein, and Rep. Sweeney) would prohibit the sale, display, or purchase of social security numbers, with limited exceptions.

[4] Remsburg v. Docusearch, Inc., 816 A.2d 1001, 2003 N.H. LEXIS 17 (February 18, 2003).

perhaps, contractual constraints to hold SSNs in confidence to ensure that they remain private."[5]

To facilitate the ready accessibility of such personal data at a time when legislators, courts, and advocates are awakening to the importance of privacy and security would be a step backward, and would be welcomed by identity thieves.

3. Intrusions To Privacy Posed by Unrestricted Data Mining of Other, Personally Sensitive Data

Protecting our social security numbers, bank information, credit card numbers, and related information will make us more secure from identity thieves and other scam artists. But other sensitive information may also merit protection. For instance, sensitive medical, personal, or family information may be referred to – or, in class action or state enforcement suits, cumulated *en masse* – within records or settlement papers. For many, the disclosure of such information can be undesirable, disruptive, and potentially harmful.

For instance, class action lawsuits against pharmaceutical or asbestos companies may contain the names and addresses of claimants suffering from a wide variety of ailments, ranging from cancer to depression. However, such claimants may have very good reasons to avoid universally exposing their chronic conditions: in the hands of an employer, the information may provide a basis for discrimination; in the hands of an insurer, a basis to deny coverage; and in the hands of a financial institution, a basis to deny a loan.

Some sensitive personal information is available today, in various forms, if one is willing to pay for it.[6] But if such information becomes even more cheaply and readily accessible and

---

[5] Id., 816 A.2d at 1008 (citations omitted).

[6] For instance, the Dunhill International List Company offers vast mailing, telephone and email lists of "consumers with ailments," literally ranging from acne and asthma to ulcerative colitis. It

searchable online – in other words, orders of magnitude more accessible than it is now – information brokers can and will aggregate and find a cheap market for the data. Large employers will purchase the data, as will banks and insurers. And the lives of those with difficult, often hidden, conditions may find fair treatment yet more elusive.

Likewise, records that reveal lists of victims of predatory lending or other frauds and scams can expose these victims to further harm. In the hands of unscrupulous marketers or lenders, this information amounts to an easily mined potential "victims list."

These are but two examples of groups who, in seeking sanctuary in the courts, may merit protection from further victimization *via* universal exposure of their records. If such groups are afforded no control over their personal, sensitive information, they may simply opt out of the judicial process. Such a chilling effect should be avoided, or at least diminished, where at all possible.

In light of the above realities, we address the Commission's specific questions below. We have listed certain questions in combination, for efficiency of reference.

(1) **In light of the recognized public interest that is served by having court case records available for public inspection, are there any privacy concerns that should limit public access to those records on the Internet?**

and

(2) **Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the internet by the Unified Court System? For example, when public court records contain an individual's Social Security identification number, credit card numbers, bank or investment account numbers, or other personal identifying**

---

lists a profile "count" of 142,316 persons with high blood pressure, 51,963 with incontinence, and 135,240 with depression. See www.dunhills.com. However, this "marketing tool" is presently relatively expensive, costing $1.00 to $2.00 per name, for a complete profile.

information, should privacy concerns limit their disclosure on the Internet?

The accessibility of court records is of fundamental importance; the interests of justice, free speech, and democracy depend on a citizenry aware of and concerned about its justice system and how its courts serve the community. In a minority of cases, however, a competing set of privacy principles – with similar goals in mind – must be weighed against online accessibility and searchability of records.

As discussed above, the privacy/security concerns are twofold. First, certain identifying information that is commonly misused should probably be cloaked in some manner. Otherwise, identity thieves will use public court databases to mine cheaply for social security numbers, banking information, credit card information, and the like. Second, highly sensitive information that might be collected or aggregated, such as by information brokers, may also require protection. As discussed above, this might, for instance, include medical or financial information – particularly where the personal information is not central to the case; one example might be records (such as in an exhibit to settlement papers or a claims administrator's report) that cumulate hundreds or thousands of claimants' names and addresses in a suit against the makers of anti-depression drugs, or heart medication.[7]

The balance between privacy and open access can be substantively affected by the types of database searches that are permissible. For instance, if full-text, open field searches are permissible, an information broker or identity thief can more easily extract social security numbers or bank accounts from a database. By contrast, if users must submit the case name or

---

[7] There might be a substantive distinction between protecting the names of such class action claimants (particularly if they are not named plaintiffs) and, say, that of an individual plaintiff in an ADA suit, particularly against a public entity.

number in order to access each case, such mining is less likely to become routine. At least two caveats to this exist, however: first, such controls do not address the concern that a specific case (say, involving mesothelioma or anti-depression drugs) will be mined for mischievous or illegal purposes; and second, regardless of such controls, court administrators may wish to design the online database with the aim of limiting circumvention by "spidering" programs, which mine the site for personal and sensitive data.

As to such "spidering" programs, it might be worthwhile to implement both technical and legal remedies to monitor or enforce unbounded or burdensome web site and server usage. For instance, some web sites intended for general public access but not for wholesale extraction – *e.g.*, resumé posting sites, including the U.S. Department of Labor's job bank – post terms and conditions of usage that prohibit data mining by commercial recruiters.

While we are unaccustomed to such conditions on the extraction of mere information, society does place restrictions on many other public resources. The public nature and purpose of a web site or database may indeed justify certain use limitations, much the same way that a public park, to serve the common good, places limits on how citizens can use it. Just as we cannot pluck flowers from the Botanic Gardens, it may be reasonable to place limits on *en masse* data mining from a public web site. Otherwise, if everyone decided to mine data (at public expense), the entire system could fail: server capacity would be burdened and the system might crash; worse, citizens might hesitate to trust a court system that conditions their assertion of rights on their disclosure of secrets to anyone with access to a computer.

(3) If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic/Internet availability?

and

(4) **If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys or by others?**

As discussed above, the types of data that might potentially be cloaked from widespread digitized access are not confined to "personal identifying information," and might include other sensitive personal information, *e.g.*, relating to health, financial, or family matters. Most likely, technical and coding solutions will need to be combined with decisions by the attorneys of record and the court. A general, but not exhaustive list of the types of information that may be redacted as of right, for use online, would be helpful. It might be necessary in some cases for two sets of documents to exist – one for online reference, and one for courtroom, or courthouse, use. The court and the parties might work together to exclude particularly sensitive information from the online record, or from filing altogether, should privacy concerns arise.

A more difficult situation arises when personal or sensitive information is submitted by the adverse party. To address this, it might be necessary to formulate a similar "as of right" list of information (medical, familial, etc.) that must be identified and/or redacted absent consent by the underlying party; a certification might be required of adverse parties, or rules adopted regarding treatment of such information. Likewise, particularly in cases involving sensitive information, it would be prudent to delay online posting until at least several days have passed – giving the object of such sensitive information an opportunity to request redaction, as appropriate.

Whatever system is selected to safeguard particularly sensitive information, there are bound to be imperfections. But the system need not be foolproof in order to reasonably

safeguard privacy – just as the present system does not prohibit anyone from copying information from court records. Rather, the primary motive in designing the system should be to provide enough safeguards and checks so that identity thieves and others do not descend in droves to excavate a public resource for harmful purposes, chilling ordinary citizens from asserting their legal rights.

(5) Should the public be charged a fee to access court case records on the Internet?

This office's position is that, as a general rule, no fee should be charged for access. Otherwise, the information provided becomes a resource more available to the wealthy. In an age when, increasingly, information is power, such an imbalance is not worthwhile. Further, given that a credit card would likely be the payment option of choice, assessing such a fee would discriminate against those without a credit card.

(6) What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or index number, or some other limited method, or should full text searches be available?

As stated above, full-text searches raise considerably more serious security and privacy concerns than isolated docket searches, geared to a specific case. For the reasons also stated above, court administrators might also wish to consider whether any conditions (or obstacles) ought be imposed on commercial vendors who simply extract these records, and permit such searches.

TRIBUNE

David S. Bralow
Sr. Counsel
(212) 210-2885

Law Department
220 E. 42nd Street
4th Floor
New York, NY 10017
Fax: (212) 210-2883
dbralow@tribune.com

HAND DELIVERY

May 30, 2003

Floyd Abrams, Esquire
Chairman
Commission to Examine Future
of Court Documents on the Internet
c/o New York State Unified Court System
25 Beaver St.
New York, NY 10004

Re: Statement of Newsday, Inc. and Tribune Company

Dear Mr. Chairman and Members of the Committee:

Newsday, Inc. and the Tribune Company are grateful for the opportunity to submit comments relating to issues that arise from providing access to court files electronically and through the Internet. Besides *Newsday*, the Tribune Company publishes 11 daily newspapers, including the *Chicago Tribune, Los Angeles Times, Orlando Sentinel, South Florida Sun-Sentinel, Baltimore Sun* and *The Hartford Courant.* It also operates 26 television stations throughout the country, including WPIX in New York and WEWB in Albany.

My name is David Bralow and as Senior Counsel for Tribune Publishing, I am pleased to take this opportunity to address the issues before this committee.

A. The Policy and Presumption of Access

As with any discussion about access to judicial records, particularly electronic copies of court records, the starting point must be the acceptance and reaffirmation of a commitment to an open and transparent judicial system. The United States Supreme Court described such openness of process as "an indispensable attribute of any Anglo-American" jurisprudence. Richmond Newspapers, Inc. v. Virginia, 488 U.S. 555, 569 (1980). But the tradition pre-dates modern observation. In 1820, when M. Hale wrote The History of the Common Law of England, (6th ed. 1820), he extolled the value of judicial transparency because: It discouraged perjury and the misconduct of the trial participants and assured that decisions were not made as a result of secret bias or partiality. Indeed, commentators as early as W. Blackstone in 1583 and J. Wigmore on Evidence in 1765 have recognized the important benefits of access to judicial proceedings and records. To Justice Oliver Wendell Holmes, the privilege that arises from reporting on judicial proceedings and access to those proceedings "stand in reason upon common ground." Crowley v. Pulsifer, 137 Mass. 392, 394 (1884).

This "prophylaxis" of access is acknowledged in every state in this country. Its recognition is rewarded by presuming access to judicial records and proceedings and by requiring those that seek to prevent access to judicial records to demonstrate a compelling interest to justify such closure.

It is our position that any debate about access to these same judicial records in an electronic form or through the Internet must be informed by the same presumption. Discrimination between byte and paper – the imposition of restrictions on one but not the other -- requires a demonstration that access to the electronic record causes a qualitatively different effect than access to the paper record. And the difference, itself -- not simply the information -- must jeopardize some compelling interest. See e.g. In re: Petition of Post Newsweek Stations., 370 So.2d 764 (1979) (this standard is a reiteration of a standard created when cameras were permitted in Florida courtrooms).

To recognize such a difference threatens the presumption of access, itself. If access to judicial records is presumed to be in the best interest of the community in which we live -- and that is not doubted -- how can permitting more convenient, more accurate access to those same records result in a compelling threat?

If anything, the removal of barriers to courthouse records empowers the citizen in a way that was arguably lost in America and reinvigorates a core value associated with public observance of the judicial system. As the United States Supreme Court recognized in Richmond:

> In earlier times, both in England and America, attendance in court was a common mode of "passing time." With the press, cinema and electronic media now supplying the representations of reality or the real life drama once available only in the courtroom, attendance at court is no longer a widespread pastime. Yet [i]t is not unrealistic even in this day to believe that public inclusion affords citizens a form of legal education and hopefully promotes confidence in the administration of justice. Instead of acquiring information about trials by firsthand observation or by word of mouth from those who attended, people now acquire it chiefly through the print and electronic media. In a sense, this validates the media claim as functioning as a surrogate for the public.

448 U.S. at 572-73, (citations omitted). By providing records electronically, the court system has the possibility of restoring direct citizen contact with the judicial system and removing a media filter.

B. Tangible Benefits to the Public and the Media

This is not to say that *Newsday* and Tribune believe that the Press's function will be made obsolete by any such direct citizen involvement. To the contrary, we believe that access to judicial records in an electronic form improves the media's ability to fulfill our mission. Electronic access increases timeliness and accuracy and offers the reporter tools to discern trends that affect society and the judicial system.

Timely examination of court records is an indispensable part of the newspaper's craft and access to the records electronically will allow greater accuracy and more complete reporting. This is true not only for long-term projects, but it is also essential for daily journalism and articles that get published on deadline.

For daily reporting, this cumbersome and out-dated means of storing and retrieving information on important judicial developments creates a news barrier that burdens the newspaper to the disadvantage of

its readers. In addition to the burden on the court personnel to retrieve and copy files, sometimes, the "hard copy" paper method makes it impossible for the reporter to gather critical information. There are numerous incidents when our reporters are stymied and the readers deprived because the court file is in the judge's chambers or in the possession of attorneys. If access were permitted online, a newspaper could rely on the court file rather than the exigencies of extra-judicial statements.

There are other logistic considerations. In Suffolk County, for instance, there are state courts in five different locations - some 30 miles apart - and court clerks' offices in two of those locations. Court personnel often cannot locate a file or even say what courthouse the files is in. A reporter or any citizen is forced to drive back and forth just trying to find the file. The same holds true in Nassau County, even though the courts are closer together - 15 miles apart at most - but anyone who has driven there knows that traffic eats up valuable time even more so than distance.

There are other problems that can be resolved by electronic access. Without the benefit of authority or a sealing order, clerks, attorneys and prosecutors remove documents from files, even in criminal cases, based on the mere belief that the document should not be public or will impair an ongoing investigation. An electronic records retrieval system will compel trial participants to seek appropriate sealing orders rather than exfoliating the file.

Electronic filing may also resolve problems with uniformity. For example, a Newsday reporter examined hundreds of Surrogate Court files to document the fees attorneys received in trust and estate cases. Sometimes, the petition for fees and the Judge's order establishing the fees were missing. While the Courts have recently revamped its rules to protect against such lapses, we believe a process whereby material submitted to the Court is immediately placed online would solve this problem.

In addition to enhancing the accuracy and timeliness of coverage of specific cases, our ability to serve the community with complete and accurate news is enhanced when full text searching is permitted. That type of functionality permits the public to locate court records applicable to particular subjects.

Access to judicial records have helped Newsday produce articles of profound impact. For instance, Newsday published a series about Catholic priests who were allowed to continue their ministries despite being accused of sexual abuse. Another series focused on the prevalence of inmates who were beaten by correction officers and the medical care of inmates at the county jails. Critical information for both series originated from court records that had to be reviewed at the courthouses by reporters. However, without access to the files online, the process was expensive and time-consuming, creating barriers both to the Press and the public. With online access and full text searching, we can do in depth reporting more often and with greater insight and accuracy.

If full search access is not economically feasible, at a minimum, we request the ability to search using names of the parties, the county, attorneys/law firms of record, case or index number. It is only with an index system that that an electronic filing system is useful.

C. Countervailing Interests in Privacy and Identity Theft

Against this backdrop which validates society's interest in an open judiciary, I do not ignore the concerns expressed about potential infringements on informational privacy and threats of identity theft. I have several observations.

First the notion of privacy must be defined with specificity before it can be addressed in a meaningful way. Privacy is an elastic concept. The unexamined trend is to distort that concept to unrealistic expectations of anonymity, comprehending even common information that is routinely found on the public street, in a phone book or on the Internet. Such an unspecified, generalized concern, cannot be the starting point for evaluating competing interests between access to judicial records and privacy. Furthermore, in New York, the notion that some information is private demands even greater attention because this State does not recognize a cause of action for disclosure of private facts.

As I stated above, before a notion of a private fact can meaningfully restrict access to a judicial record, the fact, itself, should be examined in relation to the harm caused by permitting it to reside in an open court file. This is nothing more than restating that individual judges are in the best position to protect whatever privacy right exists in any specific court files. There have always been adequate measures for

litigants and third parties to request the sealing of information based on well-established -- albeit difficult to meet -- standards. Furthermore, courts have been uniquely qualified to balance the harm against the presumption of access in case-by-case determinations. Requiring a court to determine the precise effect of online access to any specific judicial record neither significantly expands judicial labor nor requires a Court to make a decision without well-recognized standards .

A hypothetical toxic tort claim in context of Internet access to the judicial file illustrates the point. Assume that a lawsuit is filed in Nassau County against a chemical company that involves personal injury claims. The court file will, by necessity, contain medical information.

A motion to seal the file because of medical information would be evaluated on the particularized harm that arises to the individual and balanced against the necessity for public information on a subject of public importance. Furthermore, all courts recognize that when an individual seeks a remedy based on his or her medical condition, information that might be considered private in one context is no longer private when that medical condition is an integral part of the proceeding. Without some demonstration of a particularized and compelling reason for sealing, under these circumstances there would be no grounds for sealing such material. To do so, would be to ignore Craig v. Harney, 331 U.S. 367 (1947), that what transpires in a court is "public property."

The fact of the Internet and greater availability to the file cannot change the nature of the analysis. How can public information become private because a reporter now can review the court file at her office and his home? Can the public nature of this information change because of the technological advances that make access easier? I think not. But if there is some change in status that arises from greater access, the harm must be evaluated in a precise and non-speculative way. In other words, there must be some enunciated and demonstrated qualitatively different effect that arises from electronic access than that arising from access to the paper record.

This leads to the issue of identity theft. As a practical matter, I am not aware of significant problem of identity theft arising from access to judicial records. Indeed, the most common causes of identity theft are relatively low tech and do not involve court files, whatsoever.

Indeed, one cause of identity theft is rummaging through the trash for bank statements and discarded credit card offers. Identity Theft: Is there Another You?: Joint Hearing Before the House Comm. On Commerce, Subcomm. On Telecomm., Trade and Consumer Prot. And Subcomm. On Finance and Hazardous Materials, 106th Cong. 18 (1999)(statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC). Stealing a purse or wallet is another common source of the problem. Other causes are taking out false driver's licenses, creating utility accounts under another's name, establishing false bank accounts. Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Senate Comm. On Judiciary, Subcomm. On Tech. Terrorism and Gov't Info., 106th Cong. 32 (2000). In TRW, Inc. v. Andrews, 534 U.S. 19 (2001), the first United States Supreme Court case addressing the issue, a secretary in a doctor's office copied the social security number from a patient's initial referral form. In a survey of literature available, there are very few anecdotes, if any, that make a connection between judicial records and identity theft.

This is not to say that the court system through judicial rule or the Legislature through statute may not find that some information is worthy of protection. Furthermore, it is equally possible that the judicial system may seek to reform what information should be required in the court file. But before limitations on access to court files on the Internet are imposed as a general rule because of fears of identity theft, this panel should seek empirical information that demonstrates that judicial records contribute to this risk and that risk is somehow greater because of access to the Internet.

This is simply a restatement of the initial standard discussed above -- that electronic access to judicial records should only be limited when it is demonstrated that there is a qualitatively different effect than access to the paper record.

I thank you for the opportunity to provide this input and I remain available to answer any questions.

Yours truly,

David S. Bralow

Copies to:

Commission Members:

Stephanie Abrutyn, Esq.
Tribune Company
New York, NY

Yochai Benkler
Professor, New York University.
School of Law
New York, NY

Elizabeth Bryson, Esq.
Corporate Vice President,
New York Life Insurance Co.
New York, NY

Joseph Lelyveld
former correspondent and
editor of The New York Times
Bronx, NY

Christopher E. Chang, Esq.
Law Offices of Christopher E. Chang
New York, NY

Julie Domonkos, Esq.
Executive Director, My Sister's Place
White Plains, NY

William P. Farley, Esq.
The McGraw-Hill Companies, Inc
New York, NY

Maria Imperial, Esq.
Executive Director, Association of the
Bar of the City of New York Fund, Inc.
New York, NY

Pamela Jones Harbour, Esq
Kaye Scholer LLP
New York, NY

Victor Kovner, Esq.
Davis Wright Tremaine LLP
New York, NY

Hugh Campbell, Esq.
Rodman and Campbell P.C.
New York, NY

David Miranda, Esq.
Heslin & Rothenberg, Farley & Mesiti, P.C.
Albany, NY

Hon. Gail Prudenti
Presiding Justice, Appellate Division,
Second Department
Brooklyn, NY

Charles S. Sims, Esq.
Proskauer Rose LLP
New York, NY

Thomas F. Gleason, Esq.
Gleason, Dunn, Walsh & O'Shea.
Albany, NY

Norman Goodman, Esq.
County Clerk, New York County
New York, NY

Hon. Victoria Graffeo
Justice, New York State Court of Appeals
Albany, NY

Richard F. Griffin, Esq.
Philips Lytle Hitcock Blaine & Huber
Buffalo, NY

Gary D. Spivey, Esq
New York State Reporter
Albany, NY

Charles A. Stillman, Esq.
Stillman Friedman Shaw, P.C.
New York, NY

Nadine Strossen
Professor, New York Law School
New York, NY

Testimony of

Charlotte A. Watson
Executive Director
New York State Office for the Prevention of Domestic Violence

before the

Commission on Public Access to Court Records
May 30, 2003

Chairman Abrams, esteemed Commissioners, thank you for the opportunity to address you this afternoon on the most important and challenging issue of public access to court records. The New York State Office for the Prevention of Domestic Violence (OPDV) is an executive level state agency, created by the governor and legislature to improve the response of the State and local communities to domestic violence.

Great strides have been made in the past 30 years in the response to domestic violence, along with a vastly increased use of the civil and criminal justice system. The lion's share of change in the criminal justice system's response in New York State has occurred over the past 10 years under the incomparable and synergistic leadership of Governor George Pataki and Chief Judge Judith Kaye.

At the same time, the use of computers and access to the Internet has exploded. What we innocently put on the "Web" a few years ago is now being used in ways we never considered, including invasive crimes such as identity theft. We've heard horror stories of how stalking victims were tracked and harmed through information posted and available to all—for good or bad intent. We've all seen those annoying pop-up ads on our computers, advertising the ability to find, literally, anyone. As a domestic violence advocate with more than 27 years in the field, and one concerned about privacy in general, those ads, and the open, easy access to so much personal information in what we term the "information age" are truly frightening.

Nowhere is this more of a concern than when considering the safety and security of victims of domestic violence, sexual assault, and stalking. We know that domestic violence is a pervasive, on-going, life-changing reality for millions of women and children in this country, and that stalking is an integral part of the dynamic of domestic violence.

Domestic violence victims know all too well that their abusers will use any means to control and terrify them and to keep them from escaping. It is not unusual for a batterer to monitor the odometer on the victim's car, record the victim's phone calls, or use

hidden cameras. Imagine what it would be like to have a Global Positioning Satellite unit attached to your car and monitored constantly by someone in authority over you . . . this is the daily reality of many victims of domestic violence with the state of technology today. What will tomorrow hold?

It is extremely difficult and often dangerous for battered women to escape their abusers. Many find it necessary to flee the area entirely in hope of finding safety. Those who are able to get away live with the extreme fear of being found by their abuser--a losing battle for approximately 1,100 US women each year who are murdered by their intimate partners after fleeing, as well as, countless others who are re-assaulted.

There have been many attempts to help victims find safety. Recent changes in law make it a federal crime for an abuser to stalk and abuse a victim across state lines. There are processes by which victims can change their names and social security numbers, sacrificing their identities just to be safe. Unfortunately, at the same time we are recognizing the needs of domestic violence victims, the trend toward "open government" and access to information has become an easy, affordable, and valuable weapon for abusers.

As advocates for victims of crime, however, we *do* recognize the need to find ways to increase the accountability of systems, including the courts, in their responses and decisions. It is vital that these interests are balanced against victim safety and the privacy of users of our court process. In the effort to increase accountability, the court must be mindful of even the appearance of culpability should granting easy access to information result in harm to a victim. It should never be the case that potential consumers of the courts must weigh the need for safety through court intervention against the need for privacy and anonymity which may also impact safety.

In light of these concerns, I will outline a number of negative implications as well as recommendations regarding open access to court information. In addition to our own experience in responding to domestic violence, we received assistance from the National

Network to End Domestic Violence in researching this important issue. The following critical issues must be addressed before moving ahead with this process.

Negative Implications Include:

1. **A chilling effect on victims who are considering using the court for legal relief.** While we applaud the fact that family court and matrimonial records will not be subject to open access, I must emphasize that under current law, criminal court is the *only* court in which many victims may seek relief. Consider, for example, a victim who is being abused or stalked by a boyfriend. To obtain an order of protection, that victim will have to disclose significant personal information and potentially embarrassing details about the abuse in a criminal court. Under the *Conference of Chief Justices and the Conference of State Court Administrators Guidelines*, this information would be readily accessible by the public and the offender. It is not a leap to say that victims will be reluctant to pursue an order of protection under these circumstances. Is it fair to ask a victim to sacrifice her privacy for the safety she is entitled to under the law?

   Imagine the heyday the pornography and smut industry will have with such easy access to crime scene photos of horribly violent rapes and homicides. Imagine the websurfer who accidentally opens a porn site or the errant adolescent going to sneak a peek only to discover the crime scene photo of his naked mother lying in a pool of blood. At what point would the balance tip from accountability to culpability? At what price? Who and how would the decisions be made as to where to draw the line?

2. **Safety Risks for Crime Victims and Witnesses.** As I noted earlier, abusers often track and monitor their victims as a means of maintaining control. These behaviors typically increase when a victim leaves the abuser. Whenever a victim becomes involved with the court system, whether voluntarily, as a result of mandatory arrest or pro-prosecution polices or for some other reason, precious

information about her location, status, current name, phone numbers and other circumstances is disclosed. Such disclosure is a major concern for my agency and victim advocates across the state. We know that abusers will access this information and use it every way possible to stalk, threaten, assault, or kill the victim and maybe her children.

This can be a problem even when a victim is using the court system for something unrelated to domestic violence. For example, if she is involved in a motor vehicle accident resulting in legal action and the information, including the location of the court, is posted on the Internet, her address would be posted making it all too easy for her abuser to find her. Perhaps she relocates to escape the abuser and later becomes the beneficiary of a probated estate. As a result, identifying information could be posted, creating similar safety risks. Ironically, if a victim is seeking a legal name change, even this information could be posted on the Web, making her efforts at anonymity fruitless.

It's important to note that she may not be a victim at the time of her interaction with the court on the myriad of non-domestic violence related actions that could bring her to court. After one date with a stalker, she would be vulnerable to his gaining valuable information about her that could lead to her demise.

3. **Increased Opportunity for Identity Theft**. Destroying the victim's credit and reputation is a tactic already used by batterers. Open public court records will only increase the opportunity for accessing and misusing personal information.

4. **Secondary Uses of the Information.** Information stored by the courts will most certainly be used for purposes that move far from the original public policy intent of governmental accountability. It will be gleaned and sifted and compiled along with other information to create entirely new databases that can be misused and misinterpreted. Once the information is gathered for another database, it can never be taken back or corrected. In domestic violence cases, false or misleading

information could be deliberately planted by the batterer in spurious legal filings that include slanderous material against the victim which are then posted on the Web for all to see and use.

5. **Undermining Victims in Custody Proceedings.** Seeking custody is one of the most powerful tactics used by abusers to access and control their victims. Abusers will use every means available to discredit the victim and prolong a custody battle. The proposed *Guidelines* actually aid abusers in this process. Open, public access to court information provides abusers with cheap and easy access to all records of any criminal proceeding, regardless of whether such information was relied upon by the court. This poses serious ramifications for victims who ultimately leave their abusers and seek custody. Economic survival or the abusers threats or false promises often compel victims to minimize or deny the events or to later recant earlier statements of abuse that form the basis of a criminal prosecution. The fact that such records from a criminal proceeding and many civil proceedings will be within easy grasp of an abuser in a subsequent custody proceeding essentially re-victimizes the victim, rewards the abuser's use of coercive tactics, and facilitates the abuser's use of custody as a weapon of control.

6. **Dangerous Reliance on Individual Discretion**. In many instances, courts will possess far more personal information about a victim than might be held by a State agency subject to FOIL. The proposed guidelines heavily rely on human discretion and information management in an effort to protect personal privacy which will undoubtedly result in human error. Unlike many other types of crimes, in domestic violence cases, one simple failure to redact an address or social security number could have, literally, fatal consequences.
Even the most competent offices may find themselves outmatched by an abuser determined to discover the whereabouts of his victim.

Under the proposed *Guidelines*, victims of domestic violence will likely be hunted down, harassed, stalked, assaulted or even killed with greater frequency. Government exposure to legal liability will increase. It is deeply troubling for us as advocates to contemplate a system that so completely depends on individual discretion at the risk of harm to victims and their children.

We wholeheartedly agree that as much information as possible should be available to the public regarding governmental actions for systems accountability to be achieved. However, this should *not* mean full and open, cheap and easy access to everything that happens within the walls of the courthouse. We must hold this system accountable in the same way that we hold the healthcare system accountable without violating the patient's right to privacy.

There have been many recommendations made as to how to modify the proposal for open public access to court records, or to redact critical information, but we believe that none of these can ever adequately control for human error and poor decision-making, or justify the enormous expense that would be associated with such modification.

Before any final decisions are made regarding access, it is essential that there is agreement as to the goal. If indeed the objective is *governmental accountability*, then we concur with the recommendation of the Privacy Rights Clearinghouse that case information be gathered, but posted only in the aggregate, making personal identifiers unnecessary. Being able to see the number of orders of protection that a given judge issues on a monthly basis, or how many times domestic violence cases are dismissed or pled down to violations would be extremely helpful to the cause of offender and court accountability, without creating undue risks for the parties.

I would like to close with a story told by Fannie Lou Hamer that I'm sure some of you are familiar with. *Once there was a wise old man. He was so wise he could*

Testimony of
Hilary Sunghee Seo, Esq.
Domestic Violence Advocate,
Sanctuary For Families'
Center For Battered Women's Legal Services

before the
Commission on Public Access to Court Records

May 30, 2003

Thank you for giving us an opportunity to testify before you today. Sanctuary For Families' Center For Battered Women's Legal Services is the oldest and largest legal services organization in New York State dedicated to domestic violence victims. Last year, our staff and volunteer attorneys provided direct legal representation and advocacy to over three thousand battered women. We also lead community education and public advocacy efforts to help promote healthy relationships free of violence.

As citizens, attorneys and advocates of domestic violence victims, we embrace the general principle that the workings of the judiciary and court records are matters of great public interest. In a democratic society, the public not only has an interest in but a duty to inspect and hold accountable the court system. We recognize that with technological advances, there are significant potential advantages of making case files available to the public electronically – one of the main advantages being the ease with which information can be accessed.

However, ease of access also raises very serious privacy and safety issues for individuals who use the court system. By making court files available to the general public through the Internet with no significant restrictions, the courts essentially would be publishing that material to a worldwide audience. Such broad publication would provide

batterers and stalkers with a potent weapon to track down, harass and endanger victims. This is not an alarmist statement, but reflects our measured judgment based on our experience with tens of thousands of domestic violence and stalking victims and their abusers.

Why are we so concerned? I will outline our basic reasons and then go back to each to elaborate. First, we find in our work that batterers and stalkers generally are extremely obsessed with monitoring and controlling their victims. Many abusers terrorize their victims over many years, even after their victims have managed to "escape" for the time being. They often spend countless hours trying to track down their victims using any means available to them. Second, we find that the batterers and stalkers of our clients are often very savvy technologically. If court files are made available on the Internet, batterers and stalkers would spare no efforts in misusing that information to harass and endanger their victims. Third, while records from family court and matrimonial proceedings generally are not available to the public, court files from criminal and other civil cases are publicly available. Whether it be a criminal assault case involving rape or a sexual harassment case, case files will often contain personal and sensitive information about women that their batterers and stalkers could use to locate, humiliate and re-victimize them. More mundane cases involving landlord/tenant disputes or a minor car accident will likely contain some identifying information that could be used to endanger the safety of domestic violence and stalking victims. Fourth, in many cases, it will be difficult to predict beforehand what information could end up in the hands of an abuser and be transformed into a dangerous weapon. Unfortunately, once

sensitive information is released and made publicly available on the Internet, it would be almost impossible to undo the damage.

Let me now take a few minutes to elaborate on each of these points.

First, domestic violence and stalking are crimes that, at bottom, involve a desire to control and exert power over the victim. I would like to share with you the stories of two women. Both stories are rather typical of domestic violence and stalking victims, and illustrate how resourceful, thorough, and persistent abusers can be when it comes to finding ways of terrorizing their victims.

The first woman, J. S., was physically and emotionally abused by her husband. Besides beating her regularly and forcing her to have sex while he slapped her and verbally abused her, he isolated her by preventing her from working, forbidding her from leaving the house without his permission, calling her multiple times a day from his workplace to keep tabs on her, becoming angry at her if she talked to her friends or family over the telephone, and not giving her any money so that she would have to ask for his permission to buy even small items like toothpaste or feminine hygiene products. When she fled the house, he called every one of her relatives and friends until he eventually tracked her down.

The second woman, S.H., was a stalking victim. The stalker was someone she met briefly while volunteering at a community organization in South Korea. He followed her to her home one night and asked her out. When she said no, he started stalking her outside her home. He found out her work phone number and called her incessantly at work. He also stalked her at her workplace. After about a year, S.H. moved to New York to pursue her graduate studies. To her dismay, her stalker found out the name of

her school by contacting a fellow volunteer at the community organization, and took a plane and came to New York. He showed up at her school in New York causing her great fear. He also found out her phone number, email address and home address through the Internet and began to harass her. After a while, S.H. became so scared that she moved to a new location. But she is still afraid that her stalker may again succeed in tracking her down.

Like J.S.'s batterer, most abusers we encounter are obsessed with controlling and monitoring their victims. When their victims attempt to escape their sphere of domination, they often become even more aggressive and will go to great lengths to track down their victims. Like S.H., many stalking victims live in constant fear of being found out and re-victimized.

Second, in our work, we often encounter technologically savvy abusers who show enormous persistence and creativity in using the Internet to terrorize and humiliate their victims. The National Network to End Domestic Violence has observed that "the World Wide Web is far and away abusers' best tool for finding and continuing to harm their victims." It is not uncommon for abusers to spend hours scouring the Internet for potentially harmful information and spend many more hours disseminating such information to publicly humiliate their victims. To give just one example, T.J., a domestic violence advocate, had a client whose batterer was very Internet savvy. He was able to locate the confidential address of the domestic violence agency T.J. works for, even though her agency had gone to great lengths to keep the address confidential. He then created a website devoted to humiliating and terrorizing T.J.'s client and her support community. He posted the confidential address of the domestic violence agency on the

website, endangering the thousands of clients served by that agency. He also posted stories filled with what he claimed were intimate details of T.J.'s client's sex life. He did not stop there. He found T.J.'s photograph on the Internet and posted it, along with defamatory statements about T.J. using information he found about her on the Internet. This is not an atypical story. The fact is that the Internet is already a favored and extremely destructive weapon used by batterers and stalkers to terrorize and harm victims.

Third, making court records available to the general public over the World Wide Web would infuse the Internet with a large volume of information that previously was practically inaccessible except to those people willing to invest considerable time and energy to access such information. Providing electronic access to court records through the Internet is markedly different from giving the public access to those records during set hours in a set location – allowing indiscriminate Internet access would be more analogous to publishing that material to a world-wide audience and would change radically the potential usage of such information. Is such publication necessary to attain the goal of holding courts publicly accountable? Is it consistent with balancing the competing goals of public accountability and individual safety and privacy? What recourse would individuals have when such information is misused? What if the abuser resides in a foreign jurisdiction? We would urge the Commission to consider carefully these and other questions concerning individual privacy and victim safety.

While it is true that in New York, court records of matrimonial actions and family court proceedings are generally unavailable to the public, the case files of criminal and other civil cases *are* publicly available. Court records in these cases may contain

personal and identifying information that could be used by abusers to seriously harm victims. Also, New York has laws protecting the identity of victims of certain sex crimes. However, the protection does not apply unless the victim is prosecuted under very specific sections of the penal law. The identity of domestic violence victims or stalking victims whose perpetrators are prosecuted under the assault, harassment, stalking or menacing statutes would not be protected. Nor are there existing laws protecting the identities and identifying information of domestic violence or stalking victims involved in civil tort cases.

Let me give two examples to illustrate some of these points. Sarah, a battered woman, who was stalked relentlessly by her ex-husband, flees him and moves to another location. To protect her identity, she de-lists her phone number and is careful about giving out her address. She gets a new job but is terminated after she complains to her supervisor about sexual harassment and decides to seek redress in court. Her employment files which contain the name and address of her employer become available electronically because they become a part of the court's records. The case files also contain detailed information about how her boss sexually harassed her. Her batterer/stalker who is intent on finding her spends every Saturday evening scouring the Internet for information about her, and one day comes across her case. He is not only able to locate her through her work address but also threatens her that he will humiliate and embarrass her by posting all of the details of her sexual harassment case on the Internet and by mass-mailing the link to her family, friends and colleagues.

Here is a second example. Jessica is raped when she is 22. Her rapist is charged and convicted under an aggravated assault statute. Jessica testifies at the trial. Two years

after that, Jessica is sued over a minor contractual dispute. Because she proceeds *pro se* on the case, her case files contain her home address and phone number. The case eventually settles and is closed. A year later, she becomes a victim of acquaintance stalking. She tries very hard to keep him from finding her home address because she lives on a relatively isolated street, but he is able to locate her by searching electronically through case files using her name as a search word. He also finds out that she had previously been raped and begins sending her letters recounting graphic details from that case. Jessica is terrified and emotionally traumatized.

As these examples illustrate, because a woman who is currently not a victim of domestic violence or stalking could become one in the future, and a past victim of domestic violence or stalking may find herself embroiled with the courts in the future, it will be difficult to predict at any given point what information may become transformed into a weapon in the hands of an abuser.

Moreover, even with respect to more predictably sensitive categories of information, such as name, social security number, direct or indirect geographic locators such as home and work addresses, telephone number, email address and bank account information, it concerns us greatly that the guardians of such vital information would be understaffed, albeit hardworking, court personnel who may be technological novices. Also, women who have in the past been battered or stalked may in some cases ask courts to seal potentially harmful information on a case-by-case basis. But in many circumstances, they may not have the foresight or the resources to make such a petition to a court or the ability to persuade a judge that information which appears harmless on its face could potentially harm their safety. Finally, future victims of domestic violence or

stalking would have no way to undo the fact that because of cases they were a party to or a witness in in the past, there exists a body of sensitive and personal information about them that is available to the public through a court's website. Once potentially harmful information is made available on the Internet, whether because of clerical mistake or because, at the time of the posting, there was no reason to believe such information would jeopardize anyone's safety, it would be impossible to undo the damage.

We believe that the public's interest in conveniently accessing court records should never take precedence over the safety of people. We also believe that a woman should never be made to feel that in seeking redress under the law, she may be jeopardizing her safety because personal and sensitive information about herself would be made indiscriminately accessible to anyone.

I would like to end by underscoring the fact that intimate partner violence is extremely pervasive in our society. The safety issues I have highlighted are of grave concern to millions of women and the numbers are even greater when the victims' children, family members, friends, advocates and other support community are taken into account. According to a recent survey co-conducted by the National Institute of Justice and the Centers for Disease Control and Prevention, nearly 25 percent of all women in the United States are physically assaulted by an intimate partner over their lifetimes. This translates into approximately 26 million women across the nation. According to a recent survey conducted by the National Institute of Justice, about 8 percent of women are stalked over their lifetimes, or about 8.2 million women nationwide. These numbers are staggering. And as Charlotte Watson testified before you earlier today, over a

thousand women are killed each year by their partners *after* fleeing. Countless more are re-assaulted after they have supposedly escaped.

We thank and commend the Commission for the care with which it is approaching this extremely important, complex and sensitive topic. We urge the Commission to proceed with care, being mindful of the safety of the millions of women that your decisions will affect.

Thank you.

To: New York Commission on Public Access to Court Records

From: Media Law Committee of the New York State Bar Association

Date: May 30, 2003

I am Edward Klaris[1] and I want to thank the Commission for permitting me to make a presentation on behalf of the Media Law Committee of the New York State Bar Association.[2] The Media Law Committee is comprised of attorneys who specialize in issues relating to the First Amendment and privacy.[3] We represent news organizations and reporters and firmly believe online access to court records will allow for more quality journalism and improve the public's knowledge of the court system and court proceedings without compromising New York's protection of privacy interests.

Currently, searching court records is something of an ordeal; many people work or live miles away from courthouses, making it near impossible to visit the courthouses when they are open. Simply tracking down the correct courthouse in New York City can be overwhelming for reporters and members of the public trying to find information about a particular case. Electronic access to court records would allow for efficient searches of important information about attorney and medical malpractice, dead-beat parents, corporations charged with fraud, products claimed to be defective and other information that is currently very difficult to find. Moreover, not only the mainstream New York press would be able to search through court records. Out-of-state newspapers, broadcasters and websites; public interest organizations; and many others could make use of these records, causing more direct oversight of the courts and contributing to discussions of public issues.

An online database would give private citizens and non-experts access to the same material available to lawyers and government officials. As the Supreme Court noted in the Richmond Newspapers case, "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."[4] Making court records available on electronic networks would permit greater understanding of judicial decision-making, provide everyone in society meaningful access to important cases in the system and continue to improve the

---

[1] General Counsel, The New Yorker, Four Times Square, New York, New York 10036.

[2] This statement does not represent the position of the New York State Bar Assoc House of Delegates.

[3] The Media Law Committee is chaired by Slade Metcalf. The members include: Andrew Ian Bart, Richard A. Bernstein, Robin Bierstedt, Thomas M. Blair, Jennifer A. Borg, Zachary W. Carter, Jan F. Constantine, David T. Fannon, Alice L. Fradin, George Freeman, Kevin W. Goering, Michael J. Grygiel, David V. Heller, David J. Kerstein, Edward J. Klaris, Stefanie S Kraus, Richard A. Kurnit, Joel L. Kurtzberg, Matthew A. Leish, David E. McCraw, Elizabeth A. McNamara, Robert E. Moses, Eileen Napolitano, Lesley Oelsner, Nicholas E. Poser, Robert L. Raskopf, Muriel H. Reis, Madeleine Schachter, Elise S. Solomon, Katherine Aurore Surprenant, Susan E. Weiner, Jack M Weiss, Richard N. Winfield, David B. Wolf, David A. Schulz. Members serve on the committee in the their individual capacities, not as agents for their employers; views expressed herein or otherwise are not on behalf of members' respective employers, nor do the views necessarily reflect those of the employers.

[4] Richmond Newspapers, Inc. v. Virginia, 488 U.S. 555, 572 (1980).

tradition of openness that is part of the culture and law of the New York court system. These benefits are best achieved with full-text searching and easy access to all cases rather than having to input the name of the case to conduct a search.

In the context of electronic access to court records, the doctrine of "practical obscurity"[5] and concerns over privacy are misleading and do not apply. The current system of open court records works quite well and it would be a mistake to impose a new system of court secrecy in which categorical and preemptive determinations limit access. These decisions are best made on a case-by-case basis, upon a motion by the party seeking to either seal the records entirely or to curtail their availability.

The Commission is by now well aware that the U.S. Supreme Court made clear in Nixon v. Warner Communications, Inc.,[6] that the public enjoys a common law right of access to judicial records. The "presumption of openness" can be reversed only by showing an "overriding interest based on findings that closure is essential to preserve higher values."[7]

New York Rule of Court 216.1 requires judges to consider not only the parties but also the "interests of the public" and provide a written finding of "good cause" before sealing court records. The rule undergirds New York's strong public policy in favor of open court records. New York courts over the past decade have consistently relied on Rule 216.1 to deny requests to seal court records even where all parties were in favor of sealing the case. For example, in a case decided in 2001 involving the proprieties of an estate accounting and personal finances, the First Department upheld a Surrogate Court judge's denial of a joint motion for protective order to seal the settlement agreement. In that case, named In re Hofmann, the court in denying the motion noted that, even where all parties agree to seal the records, "[c]onfidentiality is clearly the exception, not the rule, and the court is always required to make an independent determination of good cause." [8]

Would the Appellate Division's analysis in In re Hofmann or other cases change if court records were available electronically? We do not think so. For decades New York courts and the legislature have rebuffed privacy advocates' attempts to create generalized privacy torts such as one for publication of private facts. On the other hand,

---

[5] Many people who fear electronic access point to the 1989 Supreme Court Reporters Committee case where the concept of "practical obscurity" was first articulated.[5] But that case has been misconstrued in the context of access to court records and ought to be disregarded by the Commission. The Reporters Committee case concerned a FOIA request for records of the executive branch, not an access motion for court records. Specifically, Reporters Committee involved FBI "rap sheets", which are multi-state summaries of an individual's criminal history and include "descriptive information, such as date of birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations."[5] Rap sheets are not documents filed in a courthouse. Rather, the FBI gathers this information from law enforcement agencies at all levels of the federal and state governments.[5] Here the public would simply have electronic access to "the source records themselves"—the same court files that are accessible today through physical inspection. Electronic access will make the inspection of public records easier. But making inspection of a public court file easier does not invade the privacy of any litigant.

[6] 435 U.S. 539 (1978),

[7] Press Enterprise Co. v. Superior Court., 464 U.S. 501, 510 (1984).

[8] In re Will of Renate Hofmann, 287 A.D.2d 119, 733 N.Y.S.2d 168 (1st Dept. 2001).

where the benefits of confidentiality in court records clearly outweigh the presumed benefit of transparency, New York already has several rules and statutes to cover this. For example, state statutes currently permit courts to seal records in family law, matrimonial and juvenile cases. The New York Public Health Law and the New York Mental Hygiene Law are the principal statutory sources of New York law that require health information to be held in confidence. Additional health-related statutes cover specific situations (e.g. HIV and AIDS patients[9], disclosure of health records in litigation[10], and the collection of statistical information by various governmental agencies). These rules would continue to apply in the electronic environment.

Congress has also passed a number of federal laws that protect certain kinds of information: HIPPA protects health information[11]; Gramm-Leach-Bliley protects financial information[12]; FERPA protects educational information[13]; COPPA protects information about children[14]; the Driver's Privacy Protection Act protects drivers' license applications and information[15]; and there are more.

With all these privacy-related laws, the chances that highly confidential information will be filed with the court in litigation have been significantly reduced. Even where such information may be turned over in discovery, only a tiny percentage of discovery information and materials are actually filed with the court, and, of course, the First Amendment does not require that non-parties be given access to discovery material that has not been filed in the clerk's office.

Perhaps the greatest fear of electronic access to court records is that information may be used in identity theft -- where a person's social security number, credit card and bank account information are appropriated and used illegally. While identity theft is a serious concern, blocking access to certain electronic court records is not the answer. Strict enforcement of the existing criminal laws and the proper implementation of state and federal privacy legislation will deter such behavior. In addition, there is no evidence that court records would ever be a good place for would-be criminals to obtain social security, credit card and bank information, while there is ample evidence that such information can be obtained elsewhere on the Internet and through criminal rings that collect the data from co-conspirators at banks and retailers. Speculative and remote fears about deviant behavior should not cloud this Commission's recommendations. This Commission should support electronic access to court records and endorse the current rule of law and good public policy in New York, which already properly balances privacy in court records with the First Amendment.

---

[9] N.Y. Public Health Law § 2134.

[10] In a court proceeding in New York, specific providers (physicians, dentists, podiatrists, chiropractors, nurses, professional corporations, medical corporations and other "person[s] authorized to practice medicine") are not permitted to disclose information which ws acquired in attending the patient and which was necessary to enable him to act in the capacity. CPLR § 4504 (rule of evidence).

[11] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (1996); 45 C.F.R. pts. 160 & 162.

[12] 16 C.F.R. § 313.

[13] Federal Education Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regs., 34 C.F.R. part 99.

[14] Children's Online Privacy Protection Act f 1998, 15 U.S.C. §§ 6501-6505.

[15] 18 U.S.C. §§ 2721-2725 & Pub. Law No. 109-69, §§ 350 (c), (d) and (e), 113 Stat. 986, 1025 (1999).

In conclusion, we suggest that this Commission recommend that New York court records be made available electronically, utilizing the same rules of openness followed by the current New York court system. Doing this will increase the efficiency of the judiciary and, correspondingly, make the records system available to all citizens so that they may monitor the integrity and efficacy of the courts. We do not request that New York expand the types of records available to the public. Rather, we simply would like New York to provide broader and more efficient access to records that are already public.

STATEMENT TO THE COMMISSION ON ACCESS TO COURT RECORDS

David Tomlin, The Associated Press

May 30, 2003

Members of the Commission, good afternoon and thank you for giving me the opportunity to appear before you today on behalf of The Associated Press.

My name is David Tomlin, and I am assistant to the president of AP at our headquarters here in New York City. Although I am an attorney and some of my work at AP is now performed in that capacity, I was admitted to the bar only a little more than a year ago. Most of my 30-year AP career has been as a journalist and news executive, and therefore much of what I will submit today for your consideration is offered from that perspective.

The Associated Press is a mutual news cooperative operating under the Not-for-profit Business Corporation Law of the state of New York. We trace our history and name to an association of New York City publishers formed in 1848. The members of this association believed they could reduce the cost of gathering news from distant locations by sharing it. It turned out to be an excellent idea that spread to other regions, and in 1901 newspapers throughout the country formed the corporation that has become today's AP.

The AP cooperative now numbers 1,700 daily and non-daily newspapers and 5,000 broadcast stations among its members. We have 147 bureaus and offices nationwide, at least one in every state. We also serve 8,500 newspapers and other customers outside the United States and maintain permanent operations in 95 countries.

We produce news reports in words, photos, informational graphics, audio and video. Our services range from international news reports in five languages, to reports that contain only the news of individual states.

Here in New York, we serve 72 newspapers and 150 broadcast stations with our New York state and New York City news reports. We have a large metro staff in New York, another substantial bureau in Albany, and smaller offices in Buffalo, Rochester, Syracuse, Garden City and White Plains.

I will begin by stating for the record that AP accepts and agrees with the general principles articulated already by other media representatives you have heard from.

We believe that constitutional, statutory and case law require a presumption of openness for all court records.

We believe that the showing demanded of anyone seeking to overcome this presumption is and should be rigorous.

We believe that when such a showing is successfully made, the restrictions to access should be narrowly targeted to the interests that have been shown to require such protection.

We believe that the appropriate way to assure that these principles are observed is on a case by case basis.

And finally, we believe that the manner of access to court records does not change these principles. What governs access to the paper records in the courthouse applies equally to electronic records accessed from a kiosk or across the Internet from a remote location.

AP recognizes that even if all these principles are accepted without qualification, the commission has many practical issues to resolve. The list of questions you have set out to frame these hearings capture many of the hardest ones.

But we see none that cannot be resolved, and we are excited by the rewards and opportunities that will ensue in the form of news reporting that can more powerfully serve both the interests of justice and the public interest.

With our statewide coverage of the news of New York city and state, and our national perspective arising from our operations in all 50 states and the nation's capital, we think AP is uniquely situated among news organizations to see where electronic access to court records can eventually lead.

We cover particular stories that emerge from proceedings in individual courthouses in every county and state. And we also produce stories that draw on information gleaned from records in dozens, or even hundreds of courthouses.

For example, AP reporters spent much of the year 2001 documenting the systematic expropriation of rural land owned by black families through abuse of the executive and judicial powers of government, and through barely concealed fraud.

The series required access to records from hundreds of courthouses throughout the southeastern United States, including civil and criminal court proceedings. It took months of reporter time and a large travel budget to do the job.

Much more recently, an AP reporter made extensive use of case files to help prove the innocence of three mentally disabled defendants in Alabama who were charged in the death of a newborn baby which it turned out never existed.

And an AP reporter is at work as we speak on a series that will examine whether changes in rates of specific crimes in the U.S. and abroad are being caused by deportation of aliens convicted of felonies. Because federal immigration authorities don't track the particular crimes that deportees committed, we need to search state court records for that information. As matters stand, much of the information we need will only be obtainable if we travel in person to where it is stored.

In all these cases and countless others, the time and expense involved is daunting. Projects that do not show at least the promise of compelling results are unlikely to attract the resources.

Simply put, electronic access to court records will produce more journalism of higher quality,

and the effect will multiply as such access spreads to more states.

Such stories are among the kinds of journalism that press freedoms are designed to encourage and protect. At their best, they can reverse injustice, increase public interest in and knowledge of the justice system, and help guide public policy makers to strengthen what works well and fix what doesn't.

We at AP know that electronic access of the volume and scope we envision will not come easily, that this Commission must consider the potential for harm to privacy interests, to public safety and to the integrity of the judicial process in developing its recommendation.

But great opportunities always come associated with some risks. Progress usually comes to those whose first determination is to seize opportunities, rarely to those for whom avoiding or minimizing risks is the paramount consideration. We hope the former spirit is the one that motivates this Commission.

Thank you again for giving AP a chance to be heard, and good luck to you in your work.

Testimony of George Freeman,
Assistant General Counsel of The New York Times Company,
to the Commission on Public Access to Court Records, 5/30/03

I am George Freeman, Assistant General Counsel of The New York Times Company, and am very appreciative of the opportunity to speak to you today. I am, of course, more than happy to answer any questions you may have.

I would start today by urging the Commission to ensure that we inadvertently do not use the opportunities technology is presenting us with to take a step backwards. What I fear the most is that because of the ready access computerized judicial records would bring, a possible -- and certainly ironic -- result might be to tilt the balance we now have with respect to all court records -- whether those in hard copy in court files, or those in electronic form -- to more closure, to more redactions and to more sealings. While privacy interests certainly ought to be respected, they are amply taken into account in the balance we have in the current regime. With the increased focus on privacy interests which the electronic world inevitably brings, we should be vigilant to ensure no pushback on the openness to judicial documents which are the very hallmark of our wonderful judicial system. The very possibility that, because of the opportunity to disseminate judicial records through the new technologies, access to records should

somehow become less public and more shielded is not only ironic, it is antithetical to the very advantages which the public can gain from the Internet.

On that point, it should also be borne in mind that any regulation aimed at electronic files may in relatively short order amount to regulation of all court files, as paper records may well disappear entirely in our lifetimes. Again, any tilting of the balance between privacy interests and openness towards the privacy end of the spectrum -- even only with respect to electronic records -- may achieve the very opposite result of the advantages to public access which the new technology offers. Since it is possible that in the future the only files that exist will be computerized, we should be very wary of creating any new rules for that medium which differ from those currently applied in our courthouses, because ultimately the Internet may become the only game in town.

Assuming, then, that we agree that the new technologies and this new initiative should not result in the diminution of openness in our courthouses, what are the advantages of a transition to electronic case files? The practical importance of the change cannot be overstated, and in most cases it is entirely uncontroversial. A paper copy of a document filed in court (i) requires a trip to the courthouse to inspect or copy once one figures out the

correct courthouse to visit; (ii) is available for such inspection and copying one person at a time; (iii) is available only during business hours; (iv) may be archived in a dusty warehouse and be hard to find only years after it is filed; (v) may be in use at trial or in chambers and, hence, not available in the clerk's office; (vi) typically can be copied only by very patient people with vast amounts of pocket change on antiquated photocopying machines; and (vii) must be manually searched for relevant information by, generally, uninformed agents for the parties actually seeking the information, and then (viii) is only truly retrievable if such party knows the exact caption or case number of a specific litigation. Clearly, access is only for the very determined and very resourceful. Electronic records solve all of these problems. We applaud the judiciary for its efforts in this area.

The notice for these public hearings suggests a limited number of areas in which restrictions on electronic access are being considered where no limitations currently exist with respect to the paper records. We view these suggestions as unwise, unwarranted and constitutionally suspect.

First, there are adequate measures available for litigants and others to request the sealing of such information in our current procedures, although the standard is, properly, a difficult one to meet. What seems quite problematic is to set up a scheme of discriminatory access, where the rules

with respect to hard records are different than those with respect to electronic records.

Before discussing why we believe the same rules ought to apply to both media, that is, why any system in which the two standards don't mirror each other is unwarranted, allow me briefly to underscore the advantages of openness -- advantages which of course are all the greater if they truly can be brought to the public rather than only those members of the public with the time, knowledge, inclination and money to actually go to a court clerk's office, a place where, frankly, I, who have litigated in New York for now some 27 years, fear to tread.

The Supreme Court's rationale in the watershed case of *Richmond Newspapers*, which stood for the presumption of public access to courtrooms and court files, applies equally to the benefits of making court records more accessible to the public. Thus,

- Ready public access to court documents promotes more discussion and understanding of the judicial system. 448 U.S. 555, 571-73, 577, n.12
- Ready public access gives greater assurance "that the proceedings were conducted fairly to all concerned" 448 U.S. at 569-70, and

serves as a check on corrupt practices by exposing the judicial process to broader public scrutiny. 448 U.S. at 570.

- Ready public access to statement made in court documents even about obsentsibly "private" matters can prevent perjury and other abuses 448 U.S. at 569 (Openness "discourages perjury, the misconduct of participants and decisions based on secret bias or partiality").

Many times, given the tension between privacy interests and access, and, indeed, in the now 16 year battle in this state about cameras in the courtroom, the participants in these struggles forget about what it is we have in common -- and that is an interest not only in the fair workings of the judicial system, but, I would submit more important, how important it is that the public perceives the judicial system as working fairly. That really ought to be paramount in any inquiry such as this, particularly in today's environment where, sadly, lawyers, judges, and the judicial system in general, are not though of terribly highly by the public -- indeed, not much more highly that even lowly journalists. Whether it be O.J., whether it be bribe-taking state judges, whether it be the perception that *L.A. Law* is the law, whether it be the lack of understanding of our adversary system and why defendants are entitled to all sorts of due process, the judicial system is not held in the high esteem it should be -- and for the very reasons

articulated by Chief Justice Berger for a unanimous Supreme Court, more openness is one important way to improve that very paramount problem.

While there has been testimony about privacy interests -- and we believe that much of the fears of openness on the Internet is more speculation than reality -- we should underscore, especially from a newspaper's point of view, the great advantages of electronic access and full-text searching capabilities. First, it would allow better reporting on the judicial system and on specific cases. A paper like The Times reports on cases throughout this big Empire State -- from Dutchess County (home of the Tawana Brawley case) to land issues in the Adirondacks, and timely and accurate reporting – relying more on court records than the spin of lawyers on the phone -- would be greatly aided if a reporter in New York had access to files in the clerk's office in Poughkeepsie.

Second, electronic access would allow improved and better reporting on a variety of matters. As one who comes from a building currently in turmoil, a problem created in part by the lack of checking with respect to an employee's background, it seems obvious that the ability for the press and public to have better access to, for example, check upon the background of potential employees is a good thing. Whether it is a newspaper being able to get access to court records about a candidate for the judiciary or any other

person running for public office; for a newspaper, or for that matter, any employer to have the ability to more easily check the true (and sworn) background of potential employees in sensitive and important professional or executive positions, there are a myriad of advantages to get more information more easily, about such high-placed people in sensitive jobs, or for that matter, about the past history of those charged with crime. Moreover, it's not just about people. Newspapers could better report about companies deceiving the public, about products claimed to be injurious, and so on.

Against these advantages, it is hard to see the disadvantages of intrusiveness. First, someone who really wants to get a lot of background about an individual, can probably do so without this new initiative. Thus, the Internet already provides access to all sorts of personal information about people, often well beyond what would be filed, and not redacted or sealed, in Court. Hence, in a very real sense, the cat is already out of the bag. Second, the balance has already been struck between privacy and openness in the standards which currently exist for protective orders, seals, and the like. Third, it is, of course, the case that in many of the fora in which potentially private information exists, the law currently permits courts to seal such records, such as in family law and juvenile cases; I'd also point out that

another area often mentioned as an area of concern, the bankruptcy courts, are federal, and hence, beyond the purview of the Commission.

Thus, I would close by saying that we believe the balance that exists now properly takes into account privacy interests as well as the great public advantages to openness, and that in embracing the new technologies, we should not alter that balance, but should welcome the added public access which the Internet brings. To the extent that the Commission believes that the rules for openness of electronic records should not exactly mirror the current rules with respect to paper documents generally, we would submit that, consistent with the Supreme Court cases, the burden must be on those favoring more restrictive rules to show a compelling reason, based on real evidence and not just speculation, on why a system that discriminates between media should prevail. If the Commission believes that such a burden has been met, the exceptions should be extremely narrowly tailored, to include only a closed, specified set of so-called identity data -- social security number, credit card numbers, bank account numbers, and nothing else -- and should be blocked from access not automatically but only upon an appropriate showing. I would reiterate that we do not think that any such discrimination is warranted, but if politically the only way to achieve the progress which the Internet makes available is by such a narrow and clearly

defined restriction, after clear evidence has been shown that it is substantially probable that real damage will occur, we could understand why such a tradeoff might be made.

Statement of Bob Port, Staff Writer, *New York Daily News*
New York Commission on Public Access to Court Records
May 30, 2003
New York, N.Y.

I have been a newspaper reporter and editor for more than 20 years, working first at the *St. Petersburg Times* in Florida, then at the headquarters of The Associated Press in New York and since July 2000 at the *Daily News*. I am also an adjunct professor at Columbia University Graduate School of Journalism, where I teach a popular elective course called "Investigative Techniques."

Since the early 1990s, I have specialized in investigative reporting that uses large databases of public records to build a foundation for accurate, probative journalism. I process electronic records, sometimes by the billions, to ferret out and document otherwise hidden connections and trends. This has yielded, for example, stories about: abusive nursing home aides employed after concealing their prior convictions for abusing the elderly; federal employees stealing horses from federal lands to sell for horsemeat; anti-smoking physicians with huge personal investments in tobacco farm land; and the involvement of all major clothing retailers in widespread illegal labor practices in New York City's garment sweatshops.

I rely on the courts, more than on any other branch of government, to be an impartial source of balanced, truthful information.

With the growth of the Internet as a digital communications medium in recent years, a cacophony of voices are expressing worry about the danger this poses to individual privacy rights. By publishing all court records on the Internet, for instance, the fearful warn, the World Wide Web could become a 'Big Brother' library. Each intimate detail of our past embarrassments will be logged for eternity. Facts once anonymous by their obscurity will join an instantly searchable database available to any faceless enemy to unjustly use against us with a mouse click on a screen.

In reality, this idea is foolishness rooted in ignorance - a modern version of killing the messenger, or in this case, a whole medium. The Internet does one thing and does it utterly democratically: It makes the transmission of information exponentially more efficient. All else that results would, or could, have occurred nevertheless. For court records, it merely saves trips to the courthouse.

I would also maintain that to attempt to make private on the Internet that which is already public on paper - like material archived by court clerks - is futile. Worse, such policies harm the public in a manner that outweighs the protection afforded any individual. Suppression of access hinders our progress, leaves our state's commerce less competitive and conceals threats to our safety that we rely on our courts to expose.

There is one and only one policy that makes sense for electronic access to court records: Information that's public at the courthouse should be available on the Internet to all for no more than its cost of publication.

To do less is to bar the common man from the real clerk's office of the future. To overcharge for access would be like selling tickets to a trial.

The status quo

Currently, I would describe New York State's online access to court records as poor. The federal courts, usually a bastion of conservatism where technology is concerned, are years ahead. The federal judiciary now has nationwide online access to dockets and other basic information available to anyone through its Public Access to Court Electronic Records (PACER) system. Fees are a modest seven cents per page collected quarterly by credit card and discounted for large downloads. Most federal districts have web access. Soon all will. A national case party name search is available and it includes all criminal indictments. Almost a third of federal courts have converted or will soon convert to a fully digital document system, where pleadings are filed electronically in Adobe's Portable Document Format (PDF), a format recognized by the Library of Congress and the National Archives and Records Administration.

The federal civil court in New York's Eastern District, home to much significant litigation, went digital two years ago. In New York's Southern District, bankruptcy court has been digital for five years. The record of the Enron bankruptcy case, including reports and many transcripts, for example, can be downloaded from the Internet on a Saturday afternoon. *The New York Times* did just that when it published a breaking Sunday report on the company's early internal investigation of what went wrong - news that rightly stunned readers everywhere and promptly intensified public debate.

By comparison, New York State courts make available only calendar entries online and only for open cases - what appears to me to be a convenience designed to aid lawyers and law firms in checking their schedules.

There are states where electronic access to court records is far worse. Mississippi is one. Alabama is another. Maine, a place where some court records still exist only on paper index cards, has a historic hostility toward computerization of government records. Had Maine's archival criminal files been automated, we might well have known earlier than a week before Election Day of the well-kept secret of candidate George W. Bush's youthful arrest for drunken driving. That we eventually learned of this case anyway is an illustration that nothing once public in court can be expected to remain hidden forever.

New York State should become a model for public access to court records on the Internet - for the health of its economy and to better inform its citizenry.

Florida, a less populous state with a shakier revenue base for its judiciary and a constitution that outlaws income taxes, manages to make electronic access widely available at cost, county-by-county, online or on CD-ROMs containing whole data sets. One can download a statewide Florida

rap sheet check (covering arrests of more than two million living persons dating back to the 1940s) through the Internet for $15 with a credit card.

In New York, a complete check of the "CRIMS" database is not available on the Internet or through any private vendor. It covers only populous counties, costs $25 and requires a visit or call to a clerk's office. This is inefficient, costly and it reduces the productivity of businesses that rely on this basic due diligence in hiring, lending or other business. It complicates the legitimate work of a free press, too. We can do better.

The privacy myth

As a journalist, what I fear most is that when New York begins to seriously publish court records on the Internet - and it will - names, dates of birth and addresses will be censored for "privacy" reasons.

Many Americans seem to assume that, by some birthright, they can expect their name, date of birth and home address to remain secret from whomever they choose, even when it was recorded because of their conviction for a crime.

This has always been a silly idea in a nation that requires citizens to serve as jurors in court. It became sillier as America industrialized and embraced inventions like the telephone, which requires telephone books. In an age of digital recordkeeping, it becomes downright stupid.

Get a clue. Names, birth dates and addresses for nearly all adult Americans are already widely available to the public through the Internet. Finance, commerce and politics depend on this.

While personal identifying information in its most accurate and detailed form is not *freely* available, that is, it is not published on free web sites, it is absolutely available at a low cost. I teach journalism students how to locate the birth date and home address of anyone in the United States in five minutes or less at a cost of about $5 per name. The only requirement is that the person has possessed a bank account or credit card (the details of which are *not* public); has received mail; has owned a car; or has registered to vote.

Information is like water. It flows to the sea via the path of least resistance. In our nation of free speech and capitalism, we reward investors who get people information they need and want. So it is with identifying facts on individuals. They will always be everywhere.

For more than 10 years, Aristotle Industries, a data vendor that mostly caters to political campaigns, has collected nationwide voter registration records. With an Aristotle internet account, and at a cost of less than $20 per search, one can call up any voter's home address or addresses; his or her date and place of birth; past and present party affiliations; and election attendance. I can see the same information for other voters who shared the same household, such as spouses and children. The information

is meshed with neighborhood demographic and religious data culled from a range of sources. This is how the Michael Bloomberg campaign, for instance, can conduct a phone survey of older white Jewish Democratic voters in Washington Heights whenever it wishes.

If Aristotle goes out of business, I assure you there will be a new capitalist venture emerge to take its place and elected politicians who will assure its right to compile records. Unless we make voter registration confidential, an un-American concept that would invite corruption, we can expect our names, birth dates and addresses to remain available through the Internet forever. It is the price of citizenship. A small price, I'd say.

There are many more examples. The federal Fair Credit Practices Act gave Americans unprecedented rights to demand the equitable availability of credit from banks. It gave creditors rights, too, such as the right to share identifying information on borrowers. The intent was a good one: to facilitate bill collection. What evolved were numerous businesses that legally sell access to databases of name, age and address histories. The data are accurately interconnected by confidential Social Security Numbers that are withheld from customers not authorized to obtain an SSN.

Congress has recently given citizens the right to request that creditors not share their identifying information, but large brokers of credit bureau data, such as Equifax, already possess so much data from so many credit accounts, and have so much other data available to them - for example, from magazine subscriptions and professional associations - that all our horses are way out of their barn. The U.S. Postal Service makes its change-of-address database available to businesses. This also assists data brokers in tracking us. What else is the post office supposed to do? If our identities are secret, how is the postman to deliver us our mail?

With computers, today's mosaic of sources, each one legally public, makes it possible to compile directory-type information on anyone, but this is not exactly top secret stuff, is it? Data brokers are civilly liable for misuse of their material. Identity theft can be vigorously prosecuted. The press cannot barge into someone's home to get a story.

This is the reality of personal identification data in the United States today. Americans who live normal lives enjoy great benefits, but must expect that their names, ages and addresses be knowable. Courts should recognize this reality and leave it to politicians to debate privacy. It is not the job of the courts to suppress public information as a prophylactic measure based on hypothetical concerns about privacy. Law enforcement authorities already have the power to pursue criminal acts violating privacy. Civil law already acts as a check on irresponsible acts by the news media or businesses.

Personally identifying information in court records should be as public on the Internet as it is in court records - no more and no less.

The court's digital divide

I suspect many judges would be surprised to learn how much of the court's business is already published on the Internet. However, what principally characterizes this material is that it is very, very expensive. As a result, a digital divide has evolved. The rich can use computers to automate their work with court records. The poor cannot afford it.

Currently, Meade Data, through its Lexis-Nexis service, is the biggest vendor of New York State court records. Every filing and every final judgment in civil court triggers a synopsis published in the Lexis-Nexis public records library. All major news organizations and any sizable business typically subscribes to this data at an annual cost ranging from tens of thousands to hundreds of thousands of dollars. Some public libraries subscribe, too, and their Nexis terminals stay busy.

New York civil docket information is available through at least two vendors, the bigger being CourtLink, which was recently acquired by Lexis-Nexis. CourtLink can supply a current docket report for any civil case at a cost of roughly $10 per search. Some corporate customers spend thousands of dollars per week for live, e-mail-based tracking of selected cases or selected categories of litigation - a kind of automated due diligence.

Competitors who might offer more affordable alternatives face a daunting obstacle: The Unified Court System's fee is $20,000 to acquire the raw historic civil data accumulated since the 1980s needed to seed a new database. Daily data transmission of updates incurs a weekly fee of $545.

I question the propriety of these fees. The *Daily News* recently acquired this data. It can be recorded on two blank CD-ROMs at a duplication cost of less than $2. Why does the judiciary charge the public $20,000?

The picture is worse for the public when it comes to criminal records. There are no legitimate private vendors of criminal data. Record checks are offered by the Office of Court Administration at $25 per name - an exorbitant fee for public records from a system paid for by the public.

One can negotiate the purchase of a copy of the "CRIMS" database from the OCA at a cost of $750 per update, but only in exchange for an agreement not to share or publish the database - so that the courts retain their ability to raise revenue by selling criminal records checks.

This is not fair. Electronic criminal records checks should be available for free or for the pennies that they actually cost. The executive branch freely publishes Department of Corrections inmate records on the Internet.

In short, New York State's courts have developed a taste for selling electronic records to generate a profit on an investment of public money in technology. The rich enjoy the benefits of automated court records while others, including many worthy non-profit public interest groups, are deprived of information they equally deserve.

While this may have its roots in the failure of the Legislature to properly finance technology for the third branch of government, the court system ought to know better. Fees based on the cost of duplication or publication would be more appropriate.

Open records on the Internet promote accuracy and truth

In the competitive news environment of New York, there is great demand to know as much as possible as quickly as possible. When it comes to old fashioned paper court records, this is a challenge.

By making basic data, and eventually court documents themselves available on the Internet, the judicial system would become a force for greater good by promoting the free flow of knowledge. People unjustly accused can have the disposition of their cases known more quickly. Questions about how many citations the city is issuing can be answered impartially, quickly and authoritatively. A corporate citizen's record on product safety can be sized up within a week or two, rather than with an impractical lengthy investigation.

Rather than representing a threat to personal privacy, open electronic records, in my experience, promote public good, public safety and healthy political debate.

New York's judiciary should get to work and go totally digital - immediately.

Comments of Stephen W. Bell
Managing Editor, The Buffalo News
Buffalo, New York

Before the New York State Commission
On Public Access to Court Records

June 12, 2003

The significance of the issue of how open New York's courts should be is borne out by Chief Judge Judith Kaye's creation of this commission, and by the distinguished members of the panel and your reputations in this field. Thank you for the opportunity to be heard.

The history of technology seems replete with examples of how the advances preceded clear societal systems, rules and customs for dealing comfortably with the innovations. The Buffalo News feels strongly that because technology will improve public access to court records, this commission should in no way restrict that access under the guise of slowing down or blunting the technology's promise.

In other words, as current real restrictions disappear – such as locating a case file in a dusty storeroom, finding a clerk to retrieve it, having a pocket full of quarters to copy the needed documents – we would urge the commission not to introduce speed bumps to the free flow of information to the public.

Newspapers – and especially their reporters – thrive in a free society where access to factual information is unhindered. Every newspaper in America would prefer to start with the unspun, unvarnished truth and write articles based on that beginning point.

As you know well, however, that is seldom the case. Reporters start with second- or third-hand sources and work their way back, hoping to get as close to the facts as they reasonably can.

New York, in its commendable protection of journalistic rights and legislative support for Freedom of Information and open meetings, has a

lengthy history of choosing openness and maintaining the public's right to know.

David Tomlin described this tradition forcefully in his testimony for The Associated Press in your New York City hearing and such universals bear repeating:

- We believe in the presumption of openness for all court records.
- We believe that anyone seeking to thwart or overcome this presumption must be held to rigorous standards.
- If that standard is met, we believe restrictions on access should be narrowly targeted to the interests that require that specific protection.
- And, we believe that "the appropriate way that these principles are observed is on a case-by-case basis."

Rules in the public's broader interest should be enacted to open or maintain public access to court records, and, in this electronic age, openness should be the "default key." The person who wants to close records has to make the case that keeping them open is damaging.

Since long experience of newspaper reporters and editors – and their attorneys – has shown that a law as written is not always a law as practiced, this commission would be well advised to lean toward maintaining and giving the public the freest possible access.

We would not urge this commission to allow public access to information that could be shown on a case-by-case basis to damage people. Embarrassment, even justified humiliation, however, should not come under the umbrella of damage.

What is of use is not just the contents of a sensational trial, but also the routine, day-to-day facts that can make reporting more accurate, thereby better serving society. Correct determination of suspects' prior criminal records, for instance, ensures fairness; after-hours access to lawsuits provides information for a complete story, rather than one based on what a plaintiff's lawyer might leak at 5 p.m. on a Friday, not that that's ever happened; and

citizens can get information to make decisions about grievances they may want to pursue against a corporation or individual, such as in class action suits.

Open records means better journalism and an enhanced level of public knowledge.

Among the other lessons that the leaps of technology have taught us is that trying to "hold back" new realities technology creates is misguided at best. Just as the typewriter inevitably made way for the personal computer, paper files will make way for databases of court information on the Internet. Your charge should not be interpreted as a search for ways to stifle or restrict the inevitable flow of such information, but how to make best use of it in a free society and to the benefit of the most people.

Even though the perception is that the media look under every rock and into everyone's life, the actual abilities of the media, as you know, are more limited. Even in a profession that deals with hundreds and hundreds of people, stories and events daily, journalists barely affect even a tiny percentage of lives in any one region. But when crucial information about one life, or case, or person, is needed, it is likely crucial and should be available in the quickest, clearest, easiest fashion possible.

Finally, since earlier I discussed the difference between the way a law is written and how it is often interpreted, let me also reassure you with an example of how journalists police themselves, in real, everyday situations.

At my newspaper and many others, we print bankruptcies and real estate transactions; we also report marriages, births, deaths and weddings; we offer news of job promotions, public honors and arrests. While most of these are routine and cause barely a ripple, we do get calls each year from people who may be negatively affected by release of this information. When we do, we consider them on a case-by-case basis and often withhold publication if we believe damaging them is real.

For instance, a sheriff's deputy may call and say he or she recently bought a house and for their protection would not want to have their address published in the real estate listings. We usually agree and omit the information. We thereby demonstrate in ways that few know a level of responsibility and common sense most would not ascribe to us.

To sum up our view, the editors of The Buffalo News would like to see continued and enhanced free and open access to court records. Sensible limits on some information that if released could cause harm makes sense. But we would urge this commission to emphasize and hold dear the public's right to know, maintaining and ensuring swift, easy and free access to court records.

The Buffalo News is an independent daily newspaper, serving eight counties of Western New York, where it is the dominant information source, both in print and via buffalo.com. A division of Berkshire Hathaway, The News has the highest penetration rate in its primary circulation area of any top 50 newspaper in the country.

Privacy Considerations and Public Access to Court Records

Testimony of William C. Altreuter, Altreuter Habermehl
Presented before the New York Commission on
Public Access to Court Records
June 12, 2003

When evaluating which court records should be available on the Internet, and how they should be accessed, we need to consider the issue of privacy, and in considering this question this Commission should assess what social expectations are, and what the realties are with respect to individuals' right to privacy.

Privacy in the United States is a paradox. People nearly universally believe it to be a fundamental right, yet we value it so lightly that we make our shopping habits available to the world for the equivalent of 50¢ off on a carton of orange juice. The "right to be let alone," as Warren and Brandeis[1] famously expressed it, may be inexorably intertwined with the right to enjoy life, but for the most part this is not a right that courts have been willing to recognize as existing in the common law. Indeed, it is somewhat remarkable that "The Right to Privacy," which has been called the most influential law review article ever written has had so little impact on any actual jurisprudence. Often cited, rarely followed, "The Right to Privacy is more an expression of wishful thinking than an articulation of any sort of binding legal principle.

New York was among the first to turn away litigants seeking a private right of action based in a common law right of privacy,[2] and little has changed since then. For example, last year, the Second Department held that banks may sell their customers' names, addresses, telephone numbers, account and loan numbers and other financial data to third parties without concern about the supposedly private nature of this information because the intrusion into the privacy of the individuals who sought to bring a class action seeking damages arising out of this activity was found to amount to no more than unwanted junk mail and telephone solicitations. The court held that this did not constitute an actual injury, stating: "Class members were merely offered products and services which they were free to decline."[3]

New York State drivers licenses bear a bar code containing information on name, age, license number, date of birth and expiration date. Bars and liquor stores routinely scan these bar codes, and there is nothing to prevent such vendor from preserving this data along with details about what and when the individual purchased.[4]

Lawyers practicing in this State have the choice of standing in lines that can stretch to the base of the steps at 60 Center Street, or obtaining a security card that makes

---

[1] Warren and Brandeis, "The Right to Privacy" 4 Harvard L. Rev. 193 (1890).
[2] *Roberson v. Rochester Folding Box Co.*, 177 NY 538 (1902).
[3] *Smith v. Chase Manhattan Bank USA* __A.D.2d__ (2nd Dept. 2002).
[4] http://schram.net/articles/barcode.html

our names and dates of birth information available to anyone with a computer and modem, or access to the public library.

The tax assessor's information on your house, and even a photograph of it, may be on the Internet. It is public information, and it is posted in a number of places. In New York City, deed records contain the purchaser's social security number. Presently this information is protected merely by virtue of the fact that it is mildly inconvenient to go to where it is kept, but it is certainly not private. Federal bankruptcy records contain a wealth of personal information, essentially all of which is available on the Internet.

Life in the 21st Century may resemble life in 19th Century Boston as respects our expectations of anonymity, but as interesting as that may be sociologically, it does not mean much when held up to reality. Samuel Warren is said to have been motivated to explore the concept of the right to privacy out of pique over the newspaper coverage of his cousin's wedding[5]; today we are concerned about identity theft. In the end, the answer is always going to be the same and privacy experts generally acknowledge this: Nothing is private. Get used to it.

Balanced against this is the absolute right to open access to the courts. Open access to court proceedings is generally recognized as being important to preserving the integrity of the legal process, and in the public interest.[6] At the same time, the public's right to inspect and copy court records is neither absolute nor unrestricted.[7] Confidentiality agreements and sealed settlements are not favored by the law in New York,[8] but provision is made for protecting the disclosure of information under certain circumstances. CPLR § 3103 provides that the court may, on its own motion, or upon application of any party, make a protective order "denying, limiting, conditioning or regulating the use of any disclosure device," and specifically directs that such protective orders, "shall be designed to prevent unreasonable annoyance, expense, embarrassment, disadvantage or other prejudice to any person...." Moreover, the statute further provides that, in the event any disclosure is improperly or irregularly obtained, prejudicing a substantial right of a party, the court may order the information suppressed.[9]

---

[5]Turkington, Richard C., and Allen, Anita, *Privacy Law,* (West, 1999), 23. This may be a jurisprudential creation myth on a par with Abner Doubleday's invention of baseball, but both stories have some value: one has given us an attractive museum in Cooperstown; and the other has given us a number of attractive turns of phrase.

[6]NY Judiciary Law § 4.

[7]Nixon v. Warner Communications, Inc., 435 U.S. 589, 597, 98 S.Ct. 1306, 55 L.Ed.2d 570 (1978), *see, also, Aetna Casualty and Surety Company v. Certain Underwriters at Lloyd's, London,* 176 Misc.2d 598 (NY County, 1998)

[8]Uniform Rules for the New York State Trial Courts, 22 NYCRR § 216.1

[9]CPLR § 3103(c). In *Lipin v. Bender*[99]84 NY 2d 562 (1994). the Court of Appeals went even further, holding that dismissal of plaintiff's action was appropriate in a situation where plaintiff's counsel, upon coming across a pile of defendant's papers in the court room, picked them up, took them back to her office, copied them, then set up a settlement

In determining whether "good cause" has been established for sealing records, a court must balance the public interest in disclosure in a particular case against the benefits to be derived by the parties from confidentiality.[10] Courts may consider a number of factors in making this determination, and are generally quite willing to evaluate whether court records may be a source of business information which could harm a litigant's competitive standing,[11] or whether public access to court records may be detrimental to the best interests of an infant or an infant's family.[12] In addition, specific statutory protections of privacy include records maintained pursuant to the Mental Hygiene Law,[13] educational records, medical and records pertaining to HIV status. These examples are not by no means exhaustive, and, indeed, the categories of information and records that are statutorily protected as "private" are so extensive that many practitioners-- and I include myself among them-- often only learn of the confidential nature of a particular record when it is subpoenaed for trial and a motion to quash appears instead of the sought after materials..

Over the history of American law the courts have balanced privacy rights and the public's right to access court records This assessment is done by the courts on a case by case basis, when authorized by statute and regulation, and by the by the legislature, when it enacts specific statutes. Some may point to the ability to disseminate information over the Internet as a justification for changing our past and current practice. However, there is no threat here. The information that people want to get is out there and can be obtained one way or another. Given our long heald predilection for making information accessible (sunlight *is* the best disinfectant), there does not appear to be any justification for suddenly making data unavailable merely because it is now more accessible. When life centered around small towns, records were readily available to one's "entire world" simply by going to the local Clerk's Office. Now that our lives and influences have expanded beyond the once cozy boundaries of daily life, the scope of possible dissemination has increased. This is not new. The circle has simply expanded. Just as the belief is pervasive that there are greater privacy rights provided for under the law than there actually are, so to is the concern about the harm which might result if personal information becomes more accessible. There is no privacy. Get used to it.

The phrase "more accessible" may be misleading and it too should be evaluated with a skeptical eye. Notwithstanding the fact that an Internet search can reveal a great deal about an individual, anyone who has ever conducted an on-line search will agree that search queries can retrieve mountains of irrelevant data. Screening the results can

---

conference in an attempt to exploit the improperly obtained information contained in the documents.

[10] *In re Estate of Hofmann*, 729 NYS2d 821 (NY Sur, 2001).

1

[11] *Crain Communications v. Hughes,* 521 NYS2d 244 (1st Dept. 1987)

1

[12] *See, e.g. Matter of Twentieth Century Fox Film Corp.,* 601 NYS2d 267 (1st Dept. 1993).

[13] Mental Hygiene Law § 33.13

become no less inconvenient than combing the Records Room of the courthouse. After all, too much information is almost worse than too little, if having too much means that time, effort, and energy must be spent sifting through mountains of data.

This is not to suggest that privacy is not something that is desirable, or that it is unattainable, but if there is going to be a fundamental change in the law of privacy, we should not try to make this happen by way of regulations which might diminish transparency and access to court records. This is approaching the problem the wrong way, and amounts to closing the barn door long after the horse has gotten away.

If identity theft is the concern, there are certainly other ways to address this, even in the current political climate. If the concern is merely that some things are more private than others, then it seems clear that the mechanisms necessary to protect recognized privacy concerns already exist, and work well. Although it is widely believed that the Internet somehow changed everything, in fact, that belief is already somewhat passé: it now appears that the Internet has changed very little. The experience of e-commerce has shown that we do not require new commercial codes to deal with cyberspace; new rules to deal with access to court records are likewise not necessary. Our legal system uses the public nature of its proceedings as a guarantee of fairness, and the its default presumption is, and should be towards transparency. Once a dispute has reached the point that the court system has been called upon to resolve it, the assumption is that the dispute is public information, if only to insure that the system operates fairly. We should work to preserve this, and I hope and recommend that this Commission draft its findings accordingly.

William C. Altreuter is a member of the law firm Altreuter Habermehl (www.althab.com). He concentrates his practice on the litigation of complex liability cases, Internet, e-commerce and privacy issues, Hospitality law; Intellectual Property, and Alternative Dispute Resolution. He is an adjunct lecturer at the University at Buffalo School of Law, and is member of the Civil Practice Laws and Rules Committee for the New York State Bar Association. In addition, he is the editor of *Outside Counsel*, (www.outsidethelaw.com), a weblog which addresses issues related to the practice of law, including privacy topics. His publications include *Use of Surveillance Evidence Poses Risk of Ethical Dilemmas and Possible Juror Backlash* (NYS Bar Journal July/August 2002); *Legal Issues in Electric Commerce*, US Reporter AIJA 2000; *Product Liability Defenses*, New York Chapter, DRI, 1992; *International Products Liability Litigation*, Co-editor and US Reporter AIJA 1997; *Summary Proceedings*, US

Reporter, Kluwer Law International 1999; *Webvertising*, Kluwer Law International, 1999; *Contractual Indemnification in New York Labor Law*, New York State Bar Journal (July/Aug 1995); *Strategies for Successful Tort Claims Defense*, Pennsylvania State University 1993. He is a graduate of the State University of New York College at Geneseo and the University at Buffalo School of Law.

Testimony of Grant Hamilton,
Publisher of Neighbor-to-Neighbor Newspapers
Before The Commission on Public Access to Court Records
June 12, 2003, Buffalo, NY

Good afternoon. My Name is Grant Hamilton and I am the publisher of four community newspaper in Erie and Wyoming Counties and a past president of the New York Press Association.

While it is predictable that a newspaper person would support better access to public documents -- and I do -- let me first tell you why I might argue an opposite position.

Many of us have had the experience of paying an auto mechanic $70 an hour for a seemingly simple repair. When we grumble about the bill, the mechanic reminds us that the rate is $10 an hour to turn the screw and $60 an hour to know where to put the screwdriver.

A good court reporter, who knows the ropes and knows the folks, knows where to put the screwdriver. By hiring that court reporter a newspaper can, in essence, sell to the public what is free to the public. Now obviously a good reporter does more than obtain records...but by protecting that inside track to information, he has something the average person wants...information they cannot access...or at least they think they cannot. And, of course, newspapers are not alone in this. Law offices, business journals, private detectives and Internet services all have the opportunity to sell public record information to the public.

If I may, let me offer one other reason a reporter might not favor good public access to judicial records. It gives the public an opportunity to more easily check the accuracy and fairness of a reporter's work.

So, in some respects, this isn't a media issue or a technology issue -- it could be considered a consumer issue. Internet access to records empowers the consumers of the legal and judicial system and the readers of newspapers.

I am certain others have discussed the potentially significant productivity improvements electronic filing and dissemination of records could bring to the legal system, and the benefits that could be seen by the educational community.

So let me briefly discuss some ways electronic access to judicial records would benefit the approximately 40,000 readers of my small newspapers. Many community newspapers, because of the economics of community publishing, have small reporting staffs. Our newspapers cover communities in three counties, a couple of dozen municipal governments, including their local courts, and several school districts. Frankly, it is very hard for us to adequately cover judicial proceedings. This leaves us in the uncomfortable position of either not covering these stories or covering them in a manner that may offer the "who what, when and where of the story" but not the "why and how." Thus the ability of our newspaper to help our readers understand the judicial system is diminished. In many of our communities only the "sensational" cases are covered by large daily newspapers with their greater resources.

There are many areas where the electronically available information would assist in our job of informing the public. Details of Article 78 proceedings come to mind. In our communities such proceedings are not uncommon, and they often relate to land use and zoning matters that are of general public concern. As you know, oral arguments are often limited in such proceedings. The ability to easily access written complaints, answers and briefs, and to read cases cited would certainly make our reporting more accurate and thorough.

Electronic access to records, especially with adequate search functions, also would provide us with the opportunity to more quickly and accurately research trends in the disposition of cases in our courts. How does one town court deal with its DWI cases as compared to another, for example? Now, I don't believe a statistical analysis of decisions is the story itself, but it may help determine if there is a story to be pursued.

There is a hazard in journalism, that if a reporter invests a huge amount of time in research it must become a story, even if it isn't a story. There is a hazard that a reporter researching a story based on certain premise will find enough information to support the premise and miss the information that would refute it. The ability to quickly and accurately do research -- at all hours of the day -- is important in obtaining complete information and to avoid the time-is-story temptation.

Equally important, electronic access would enable editors to check facts and verify stories.

Also, especially in small towns, there is often a perception that there are people who may receive special treatment in the judicial system. It is not easy to prove or disprove such allegations, thus rumor mill can, without justification, undermine confidence in the system. The ability to quickly research such allegations could help allay those rumors, or in rare cases, prove the malfeasance of a local justice.

The ability to do story research that involves public records is an important function of newsgathering. Enabling that to be done more efficiently extends our capability, improves our accuracy, and gives our readers an opportunity to check our credibility. I believe that serves our readers and our society.

Fortunately this discussion, as I understand it, is not about making records public. That issue has been largely resolved legislatively and judicially. There is plenty of guidance as to what records are not public, leaving us with the presumption of access to most records.

There is concern that there may be legitimately private information contained in records that could be abused if easily available to the public. It's a reasonable concern and, while the same abuse is possible with hard copy records in the courthouse, I certainly support the concept that information such as an individual's social security number and credit card and bank account numbers should be given special consideration.

The key is not to restrict all information, but rather to design a system with the minimal necessary controls and to strengthen and enforce penalties for those who abuse it. When New York State replaced the winding state highways with the Thruway to improve transportation, there certainly was the possibility that there would be those who would travel at an unsafe speed and put others at risk. We didn't abandon the concept of the Thruway or restrict its use to a chosen few. We set reasonable speed limits and enforced them.

In general there should be no different rules for Internet access to court records than exist for paper records at the courthouse.

I'd like also to just briefly, provide a testimonial to the usefulness of the Internet. As you know New York State laws are available on-line. Prior to that time, in order to read a law I had to go to our local police station and borrow a McKinney's book -- that was only available to me from 9 to 5 on business days. And, not being an attorney, I wasn't always sure in what section of the code to look. Now I can read the law 24 hours a day, seven days a week and I can more quickly move from chapter to chapter to find what I need.

In addition to my newspapers, I also publish a stock market newsletter. At one time obtaining public information about public companies was time consuming and costly. Those who could afford to have a physical presence at the Securities Exchange Commission could obtain the information. That information (which, by the way, includes names, addresses and financial information about individuals) is now available to me in real time through the SEC's Edgar system. If you haven't visited the site, it has become quite "user friendly" to the general public. (http://www.sec.gov/edgar.shtml)

I recognize that there is a cost to the taxpayer to create digital records. I believe that cost will be more than offset by the productivity savings it will create in the legal system.

More importantly, however, is the premise that information is the lifeblood of democracy. While those of us who have better access to information may wish to protect that franchise, making information available more citizens can only strengthen the democracy.

Thank you for your attention. I have provided copies of my testimony and it is also available on-line at the East Aurora Advertiser website. (www.eastaurorany.com, the Advertiser section on the left navigation bar under "testimony".)

I would welcome your questions.

COMMERCIAL AND FEDERAL LITIGATION SECTION
NEW YORK STATE BAR ASSOCIATION

Comments to the
Commission on Public Access to Court Records

These Comments are submitted by the NYSBA's Commercial and Federal Litigation Section ("the Section") to the Commission on Public Assess to Court Records ("the Commission").

In April 2002, Chief Judge Judith S. Kaye formed the 23-member Commission, under the chairmanship of Floyd Abrams. She asked the Commission to examine what she described as sometimes competing interests of privacy and open access to information in court case files, in order to help shape the state judiciary's policies concerning future availability of court records on the Internet. She noted that

> In keeping with society's increasing reliance on technology, the court system will begin to make case files available electronically within the next few years. But while providing greater access to this information, we also must be diligent to protect a litigant's right to privacy. We recognize that court records can contain sensitive information, such as social security and home telephone numbers, tax returns, medical reports and even signatures. I have charged this commission with the hard task of examining any potential pitfalls, weighing the demands of both open access and individual confidentiality, and making recommendations as to the manner in which we should proceed."

Judge Kaye's announcement quoted Chief Administrative Judge Jonathan Lippman to the effect that "subjecting case files that sit in practical obscurity in a dusty courthouse basement to the large-scale, high-speed searching capabilities of the Internet raises difficult questions regarding individual privacy rights, as well as concerns over how to prevent the misuse of private data."

Chairman Abrams opened the first of three public hearings held early this summer by observing that all the issues before the Commission "relate to the question of whether internet access should lead us to take greater care, different steps, to protect privacy and other interests so as to accommodate those interests without overcoming the genuine and constitutionally rooted interest of the public in knowing about judicial records and what's in them." He noted that not all case records are now public, citing records in matrimonial matters, child custody proceedings, presentencing reports and memoranda, documents containing HIV-related information or the identify of victims of sexual offenses, and other documents filed under seal. He pointed out that the Commission's mandate is not to revisit existing rules and policies making such materials confidential, but, rather, to focus on the interplay between currently public records and the Internet and its technological successors.

Our Section's Recommendations

Our Section welcomes both electronic filing of court documents and remote electronic access[1] to otherwise public court case records, including records which currently exist only in paper form. Both developments should benefit not only the general public, but especially the bar itself. In many parts of New York (including Manhattan), lawyers' offices are often miles away from the nearest county, state or federal courthouse. Moreover, increasingly, lawyers maintain home offices and should

[1]By "remote electronic access," we mean access by computers other than the ones physically located at the courthouse.

not be required to commute to court to obtain access to judicial decisions and other court records.. And no matter where lawyers work, they routinely require access to decisions by courts located in other jurisdictions.

We acknowledge that to the extent remote electronic access sweeps away obstacles heretofore imposed by the inconvenience of obtaining courthouse access to paper records,[2] such access heightens legitimate concerns about personal privacy, confidential business information, bulk data mining, identification theft, and other sensitive matters. But we are convinced that the federal courts' substantial experience with the PACER system and with privacy rules developed in conjunction with electronic filing demonstrate that these concerns can be satisfied. Moreover, these federal programs should serve as a model for how the state's judiciary should proceed.

A. There is no "constitutional presumption" in favor of press and public access to all court documents, whether paper or electronic

We start by pointing out that the issues before the Commission are matters of policy, not constitutional compulsion as some have argued.

---

[2]George Freeman, assistant general counsel to The New York Times Company, testified that these practical considerations include the need for a trip to the courthouse, access limited to one person at a time during courthouse business hours, the necessity of coming to the courthouse armed with the precise caption or case number, the difficulty of tracking down documents to a particular file in a dusty warehouse, the possibility that the desired document is unavailable because it is in use in a courtroom or in chambers, the requirement of a manual search often by an relatively uninformed agent, the necessity for pocketfuls of change, and the handicaps imposed by antiquated photocopying machines. He acknowledged that "Electronic records solve all of these problems."

Not surprisingly, some media representatives have argued to the Commission that any and all restrictions on remote electronic access are "unwise, unwarranted and constitutionally suspect." In support of that position, they assert the existence of what they describe as a "constitutional presumption of access" supposedly established by *Richmond Newspapers, Inc. v. Virginia,* 448 U.S. 555 (1980). With all due respect, that misreads *Richmond Newspapers,* for neither that decision nor its progeny support such a presumption.

Richmond Newspapers decided, over then Justice Rehnquist's dissent, the relatively narrow question of "the right of the public and press *to attend criminal trials.*"[3] When the Court next spoke to this issue, in *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982), it overturned a Massachusetts law interpreted to *require* exclusion of the press and public during testimony of a minor victim of an alleged sex offense. In doing so, it expressly reaffirmed that *Richmond Newspapers* dealt only with public and press access to criminal trials. Justice O'Connor, concurring, noted that "I interpret neither *Richmond Newspapers* [nor today's decision] to carry any implications outside the context of criminal trials." (457 U.S. at 611) Chief Justice Burger (the author of *Richmond Newspapers)* and Justice Rehnquist dissented from what they saw as the majority's too "expansive interpretation" of *Richmond Newspapers,* and from "its cavalier rejection of

[3]Media representatives had challenged the trial court's decision, made at the defendant's request and with the prosecution's consent, to close a criminal trial to public and press. The trial judge issued no findings to support his decision.

the serious interests supporting Massachusetts' mandatory closure rule." (457 U.S. at 613) Two subsequent decisions, in the two *Press-Enterprise* cases, modestly expanded *Richmond Newspapers* – but still in the narrow context of the criminal trial process. *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501 (1984), upheld access to voir dire examination of potential jurors in a criminal trial, absent findings that would justify closure in a particular case. *Press-Enterprise Co. v. Superior Court,* 478 U.S. 1 (1986) (*Press-Enterprise II*), upheld press access to transcripts of a preliminary hearing in a criminal case. Justices Rehnquist and Kennedy dissented from even that modest extension of *Richmond Newspapers*.

As to public or press access to court records generally, the Supreme Court has found only a *non-absolute common law right*, not a constitutional one.[4] The leading case is *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978), argued by the Commission's chairman, where the Supreme Court denied media access to Presidential tapes portions of which were published to the jury and those present in the courtroom, and marked as exhibits during the criminal trial of Presidential aides, including former Attorney General John Mitchell. Written transcripts were given to the jury, as well as to reporters covering the trial, and were widely reprinted. The media then sought permission to copy, broadcast and sell those portions of the tapes played during the trial. Although the

[4]Even where, in the cases cited above, the Supreme Court has found a constitutional presumption of access, it acknowledges that even that right is not "absolute," and can be curtailed in appropriate circumstances.

Justices acknowledged existence of a common-law "general right to inspect and copy public records and documents," (435 U.S. at 597) they held that this common-law right was not absolute, and – in language directly applicable to the present Commission's assignment – ruled that

> Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes. (435 U.S. at 598)

Among those "improper purposes," said the Court, was the intention to use them "as sources of business information that might harm a litigant's competitive standing." (*Ibid*) Refusal of the media's request, said the Justices, was justified both as a matter of the trial court's discretion, and because of the applicability in this particular case of the Presidential Recordings Act. Not one of the nine Justices referred to any *constitutional* presumption in favor of public access to these court documents.

Moreover, in *United States Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989), in refusing to grant press access under the FOIA to Justice Department rap sheets containing criminal records, the Supreme Court made two important points which address arguments now advanced in favor of overriding privacy interests in favor of unrestricted remote electronic access to court records.

First, Justice Stevens' opinion for the Court rejected what it characterized as a "cramped notion of personal privacy" – that because a particular "hard-to-obtain" fact about a person has become public or is otherwise "findable," all enforceable privacy rights

as to that fact are forfeit. (489 U.S. at 763-65, 767-69, 770). Stevens concluded with a quotation from a Rehnquist speech, stating that the fact that

> an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information. (489 U.S. at 770)

Second, the Court pointed out that technology *does* make a difference:

> Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information. (489 U.S. at 764)

In short, the Supreme Court's decisions do not support a constitutional presumption of public or press access to court documents – as opposed to the right to attend important phases of a criminal trial. The State's judiciary is, therefore, free to develop rules which, in its judgment, strike a proper balance between the public interest in remote electronic access to court documents and legitimate privacy and other confidential interests – based upon good public policy, free of any supposed constitutional compulsion.[5]

---

[5]Our state courts, too, recognize the existence, not of any constitutional presumption of access, but of a non-absolute common law right, subject to judicial limitation. A striking illustration is *Danco Laboratories, Ltd. v. Chemical Works of Gedeon Richter, Ltd.*, 274 A.D.2d 1, 711 N.Y.S.2d 419 (1st Dept. 2000), where the Appellate Division struck a careful balance between media interest in court records concerning the so-called abortion pill, on the one hand, and the parties' interest in protecting trade secrets and the privacy of individuals involved in its manufacture and distribution After discussing the Supreme Court decisions cited above, the court remanded with instructions for appointment of a Special Referee to redact from the sought-after court records all information involving trade secrets and the identify of individuals involved in manufacture and distribution.

B. The Commission should recommend adoption of the equivalent of the federal PACER system and, in connection with electronic filing, privacy rules similar to the federal guidelines

The model for remote electronic access to court records is the federal Public Access to Court Electronic Records or PACER system. Access is available to anyone with a personal computer and internet access[6] who registers and opens an account with the PACER Service Center maintained by the Office of the United States Courts. Registered users are able to obtain access to information from the federal appellate, district and bankruptcy courts, via a national case index. Once a case is located, the registered user connects with the PACER system operated by the particular court in which the case is or was filed. Among the data available are: lists of parties, their counsel, judges and trustees; docket sheets with a chronological listing of events; claims registries; appellate opinions; judgments or case status; and types of documents available. Case records are currently stored in graphic format – i.e., .pdf, .tif, etc. This feature limits so-called "data mining," because to "mine" such graphic files, they must be captured, converted to text files, and then scanned.[7] Relatively inexpensive per-page charges are required, with somewhat higher charges for graphic documents.

---

[6]For those lacking internet access, dial-up access by modem is also available.

[7]We are informed that the largest users of PACER are commercial entities that do "mine" data (most, bankruptcy data), but that so far no privacy or similar problems have arisen.

As for electronic filing, the federal courts have adopted special privacy rules, restricting the kinds of personal information which can be included in electronically filed pleadings and other court documents. Excluded are full Social Security numbers, the full names of minor children, and full bank account numbers. Similar protections can be implemented in New York by amendment to the CPLR.

C. Should it propose priorities, the Commission should push, first, for remote electronic access to all judicial opinions, to the same extent they are publicly available at the courthouse

Should the Commission deem it desirable to propose a system of priorities, we believe that the most immediate priority should be given to establishing remote electronic access to all opinions by state court judges.

First, this is the bar's most compelling need.

Second, this is the least controversial form of remote electronic access. The public, after all, helps pay for and has a legitimate interest in the work of the judiciary, and should have the benefit of remote electronic access to judicial opinions that are otherwise available by physical access at the courthouse, in the pages of the *New York Law Journal* and comparable publications, by paid subscription to services like Westlaw and Lexis, and by access to existing official and unofficial web sites. And of all court documents, judicial opinions are the ones least likely to contain information raising concerns about privacy,

trade secrets, confidential business information, and other sensitive matters.

Third, this makes practical sense. The bar, the press and public already have free access by Internet to websites maintained by our Court of Appeals, all four Appellate Divisions, the United States Supreme Court, the federal appellate courts, the various federal district courts (although not all district judges participate), and the appellate courts of other states – all of which typically make opinions available on the day they are rendered. And to this extent, the state's judiciary already has first-hand practical experience in making opinions available online.

What's missing are the decisions by the state supreme court justices and other lower state court judges.[8] Remote electronic access to judicial opinions should not be limited to persons who subscribe to relatively expensive services like the one operated by Lexis-Nexis – although we believe the charges required by the PACER service do represent an acceptable way to pay for the costs necessarily involved in providing the service.

Given the state judiciary's hands-on experience with making its appellate opinions promptly available online, it should not be difficult to establish procedures whereby

---

[8]Also missing, from the websites now maintained by the Court of Appeals and the Appellate Divisions, are briefs and other papers filed by the parties.

There is no reason not to make appellate briefs available online. Submissions filed in the United States Supreme Court by the Solicitor General's Office are now available on that Office's office website; other Supreme Court briefs, on FindLaw's Supreme Court Center. Websites offering free copies of briefs in various appellate courts, including five state supreme courts and the United States Courts of Appeals for the Seventh and Eighth Circuits, are listed in "Web Watch: Free Briefs," by Robert J. Ambrogi, *Law Technology News* (July 2003), available online at www.lawtechnews.com.

decisions by supreme court and other lower court judges are created and transmitted electronically so that they, too, may readily go online.

The cost of doing so should be deemed an integral cost of the court system's operations, equivalent to filing paper copies with the County Clerks, and borne principally by the taxpayers and secondarily by the users of the courts through enhanced filing fees.

SUMMARY

Our Section welcomes both electronic filing and remote electronic access to court case files. The bar, as well as the press and public, will surely benefit from both developments. To protect privacy and other sensitive matters, we recommend the models afforded by the federal PACER system and by the privacy rules adopted by the federal courts in conjunction with electronic filing. To the extent the Commission assigns priorities, we believe that the most immediate priority should be given to making all otherwise public judicial opinions promptly available online.[9]

July 2003

---

[9]This report was prepared for the Section by the following members of the Section's Executive Committee: Carol E. Heckman (who served as chair), Daniel P. Levitt and Peter J. Pizzi.